2002-09

Windows XP Operating System security analysis

Goktepe, Meftun.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

WINDOWS XP OPERATING SYSTEM SECURITY ANALYSIS

by

Meftun Goktepe
September 2002

Thesis Advisor:	Richard Harkins
Second Reader:	Cynthia Irvine

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: **Windows XP Operating System Security Analysis**			**5. FUNDING NUMBERS**
6. AUTHOR(S) Goktepe, Meftun			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Windows XP, released in October 2001, brought new features to improve the work environment throughout organizations. The purpose of this research is to determine if Windows XP, when used as a workstation operating system in domain- based networks, provides adequate security policy enforcement for organizations. In this research we performed a security analysis of the Windows XP operating system, assessed its vulnerabilities and made recommendations for XP configurations and use as an extension of enterprise network. In order to analyze Windows XP, we set up a Windows 2000 Server based-domain. Windows XP was installed on one of the workstations in the domain. In this lab environment, the security architecture and all new security features of Windows XP have been analyzed. Then we made vulnerability scans to assess the security of Windows XP in three configurations: after clean installation, after applying current patches and updates, and after applying security templates. Windows XP comes with selectable built-in templates. A new security template was created by combining the best of these templates. The new template also contains additional security settings not found in the built-in templates. This study provides recommendations for secure Windows XP configuration in Windows 2000 domains.

14. SUBJECT TERMS Windows XP, Computer Security, Operating System Security, Windows XP Architecture, Windows XP Security			**15. NUMBER OF PAGES** 126
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

WINDOWS XP SECURITY ANALYSIS

Meftun Goktepe
First Lieutenant, Turkish Army
B.S., Turkish Army Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Author: Meftun Goktepe

Approved by: Richard Harkins
Thesis Advisor

Cynthia Irvine
Second Reader

Dan Boger
Chairman,
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Windows XP, released in October 2001, brought new features to improve the work environment throughout organizations. The purpose of this research is to determine if Windows XP, when used as a workstation operating system in domain based networks, provides adequate security policy enforcement for organizations. In this research we performed a security analysis of the Windows XP operating system, assessed its vulnerabilities and made recommendations for XP configurations and use as an extension of enterprise network. In order to analyze Windows XP, we set up a Windows 2000 Server based-domain. Windows XP was installed on one of the workstations in the domain. In this lab environment, the security architecture and all new security features of Windows XP have been analyzed. Then we made vulnerability scans to assess the security of Windows XP in three configurations: after clean installation, after applying current patches and updates, and after applying security templates. Windows XP comes with selectable built-in templates. A new security template was created by combining the best of these templates. The new template also contains additional security settings not found in the built-in templates. This study provides recommendations for secure Windows XP configuration in Windows 2000 domains.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Richard Harkins who has helped me in many ways during this research.

Also, I would like to thank Prof Cynthia Irvine for her technical support and assistance in writing this thesis.

I. INTRODUCTION TO WINDOWS XP PROFESSIONAL OPERATING SYSTEM

A. INTRODUCTION

Microsoft released the Windows XP Professional operating system in October 2001 as a replacement for Windows 2000. Windows XP was designed to integrate the strengths of Windows 2000, such as security, manageability, and reliability, with the best features of Windows 98 and Windows Millennium. This includes features like Plug and Play, and new user interface. (In this thesis, "Windows XP" refers to Windows XP Professional unless otherwise indicated.)

Windows XP not only combines consumer and corporate line of operating systems codes but also introduces new functionalities including new security features. Windows XP has been build upon Windows 2000 that has already proved some robust security features in domain networks. The new features and improvements can be summarized in the Table 1 below.

FEATURES	IMPROVEMENTS
Intelligent user interface	Fast User Switching, new Visual Style (Redesigned start menu, search companion, new my documents, webview and file grouping)
Digital media support	Windows media player, windows movie maker, digital photo support
Greater application and device compatibility	Improved device installation, supporting new hardware technologies, native support for DVDs and CDs, application compatibility, COM and shared DLL isolation support
Enhanced file and print services	WebDAV, disk defragmenter , encrypting offline files database, FAT32 on DVD-RAM,
Improved networking and communications	Universal plug and play, Internet connection sharing, home networking wizard
Integrated help and support	Remote assistance, troubleshooting tool
Improved mobile computing	Remote desktop and terminal services, power management
Reliability	Driver rollback, system restore, automated system recovery, autoupdate, dynamic update
Manageability	Intellimirror, group policy, migrating files and settings, account management and regional options enhancements
Security	Internet connection firewall, controlled network access, software restriction policies, Microsoft Passport, credential management, encrypting file system, secure data storage on the internet

Table 1: Windows XP improvements and new features (after [Ref. 1])

More information about Windows operating systems can be found in Appendix A.

Today many organizations employ the Windows 2000 operating systems on workstations in their networks. Windows 2000 Professional offered users several benefits including; stability, reliability, security features and better memory management. Windows XP touts more robust security features as an answer to business requirements to protect sensitive data and resources on the network. Putting Windows XP into a Windows 2000 Server environment offers administrators some new options including:

- Security settings
- Policy settings
- User and group management capabilities throughout an organization

Windows XP also offers thousands of security-related settings that can be implemented individually. It comes with 212 new policy settings, along with the 421 policy settings shipped with Windows 2000. The Windows 2000 policy settings are fully supported and, most of them improved in Windows XP [Ref. 2]. Administrators can simply import these policies to the Group Policy in Windows 2000 server domain controller and implement them throughout the organization.

> New policy settings only work on machines running Windows XP and will be ignored by all machines running Windows 2000. In addition, machines running Windows 2000 cannot be harmed by any of the new policies that ship with Windows XP [Ref. 2].

Although there are many new security features that can be configured by the Security Settings node in Group Policy, there are also some other new security features to be configured by other means in order to ensure an effective level of security in the organization. These features include Remote Desktop, Remote Assistance, and Encryption File System (EFS).

B. PURPOSE

The purpose of this research is to determine if Windows XP provides adequate security policy enforcement for organizations to be used as a workstation operating system in domain- based networks. We will conduct a security analysis of the Windows XP operating system, assess its vulnerabilities and make recommendations for secure XP

configurations and use as an extension of an enterprise network. Here we assume that the organization has already deployed Active Directory services, and that there will be client machines using Windows XP, as well as the other client machines using Windows 2000.

Although Windows XP introduced or improved many features, the main focus of this thesis will be security and security related features. Also as we are concerned with only domain specific configurations; some new security features that are not available in domain environments will be excluded or only explained briefly.

C. ORGANIZATION

To analyze Windows XP security, we created a lab environment simulating an organizational domain. This domain includes a Windows 2000 server, a Windows XP client, and a Windows 2000 client.

This thesis will provide analysis, assessment and recommendations for the deployment and configuration of Windows XP in existing Windows 2000 domains. Background information and a comparison of Windows operating systems are presented in this Chapter. A detailed discussion of Windows XP architecture as well as its security architecture is discussed in Chapter II. To analyze and assess the security features of Windows XP we set up a simulated network in the lab. This is explained in Chapter III. Later, in Chapter IV, the security analysis, vulnerability assessment and experiments are discussed. The results are explained and discussed as well. Finally, recommendations for security configurations and domain use are discussed in Chapter V. Here we present a recommended security template for Windows XP based on the lab analysis. This template provides enterprise security settings for computers that exist in a Windows 2000 domain. Finally, additional security configuration recommendations that can't be set by this template are presented.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WINDOWS XP OPERATING SYSTEM ARCHITECTURAL OVERVIEW

A. INTRODUCTION

To properly understand security, we need to look at the architectural design of Windows XP. There are some important changes compared to prior versions.

B. WINDOWS XP ARCHITECTURE

Microsoft's Windows XP design is a significant improvement over Windows 2000, combining the best features of client/server and microkernel architectures.

Figure 1 is a graphical representation of the system architecture.

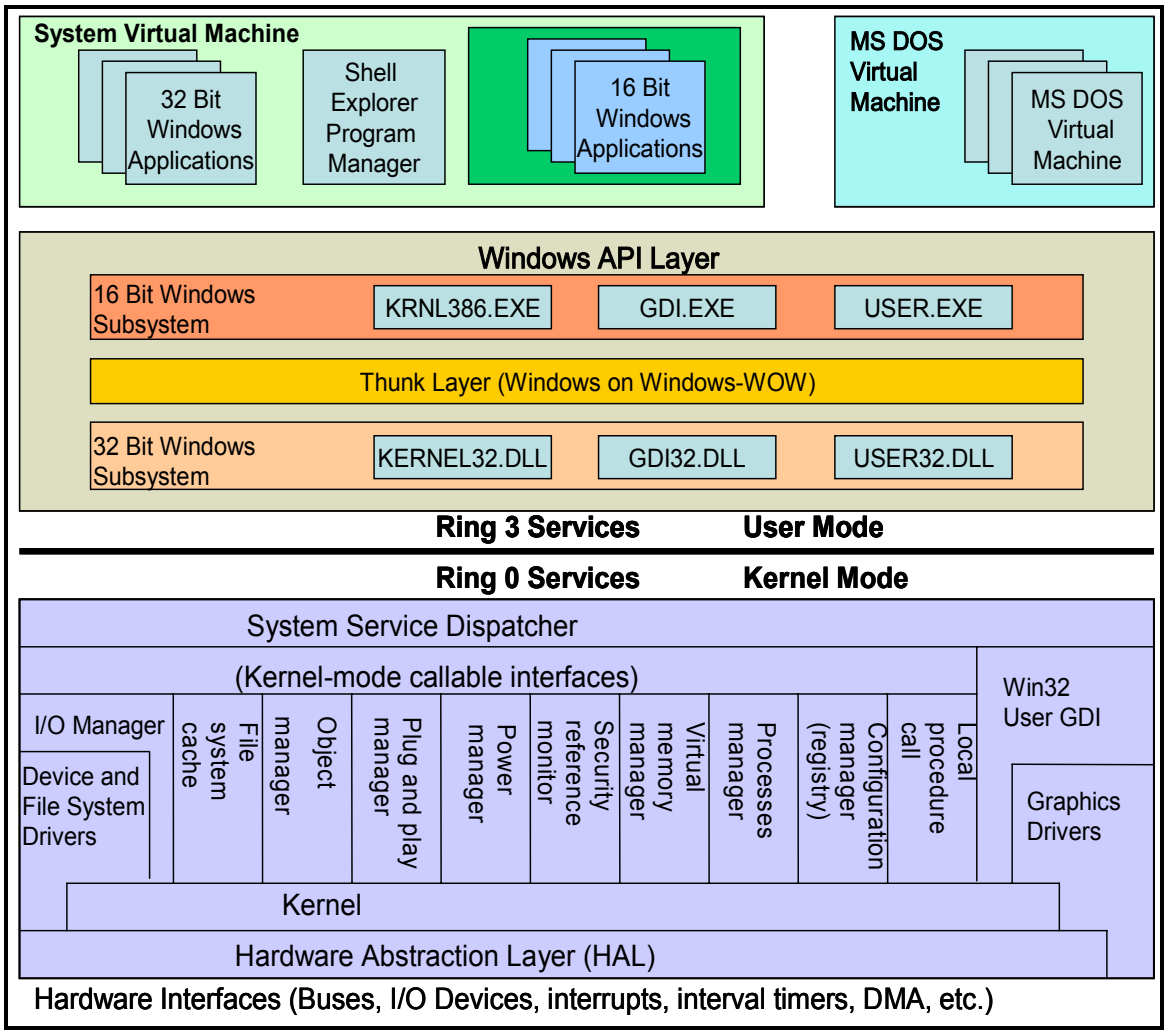

Figure 1: Windows XP Architecture (after [Ref. 3])

1. Improvements in the Windows XP Kernel

The kernel changes in Windows XP are not that many when compared to the changes made in Windows 2000 kernel over Windows NT kernel. Windows 2000 kernel version is 5.0. Because of the small number of changes, Windows XP kernel version is named as 5.1, not 6.0. But there are several important changes that improved performance in Windows XP. [Ref. 4]

If we look at the security perspective the major improvements are listed below:

a. Registry

The redesigned Windows XP registry code provides larger registry size and faster registry queries. These registry changes improve performance in the following areas [Ref. 5]:

- Converting a delayed close table to a Least Recently Used (LRU) list.
- Reducing Kernel Control Block (KCB) lock contention with do not lock registry exclusive and do not touch volatile information.
- Providing a security cache to eliminate duplicate security descriptors.

Windows XP uses new algorithms to reduce registry fragmentation, keeping related registry files closer, in order to allow faster reads. Registry memory has been moved from kernel memory space, which is basically known as paged pool, to system cache in order to increase capacity. Now Cache Manager provides the memory for registry. [Ref. 6]

b. Device Drivers

To prevent incompatible or malicious drivers from crashing systems, Windows XP verifies third-party drivers when installing them. If a driver hasn't passed Windows Hardware Quality Lab (WHQL) test, Windows XP gives a warning and can block the driver. Drivers that are not signed may still work, letting users continue the installation. This means that Windows XP does not guarantee that device will work with this driver. However when the user tries to install an application with a hard-blocked

driver, which is listed in a database in Windows XP, the user is referred to a Microsoft web site for further information. [Ref. 6]

Windows 2000 limited device drivers to 220MB. This means that users can install as much as 220 MB of device driver data in the registry. Device drivers on Windows XP can now be as much as 960MB of data. The storage capacity of the registry to store device drivers is directly related to the size of virtual address space. Now Windows XP can describe 1.3GB of system virtual address space. 960MB of virtual address space is contiguous and can be used for device drivers. Windows 2000 has 660MB virtual address space, 220 MB of which is contiguous. [Ref. 4]

Windows XP also includes System Restore functionality, which lets user return the OS to its stable states before the driver was installed. Windows XP does this by creating restore points during normal operating times by backing up system data especially before installing applications or device drivers. If the system becomes unstable after these operations, the user can return to previous stable states. [Ref. 4]

c. DLL Files

Windows XP has also improved the storage and usage of DLL files. Previously, only one copy of a specific DLL was allowed in memory at a time. If an application is installed, it might also install a new version of a DLL, replacing any earlier version in the same directory. Thus, applications using older DLL files might not work. Windows XP allows more than one version of a DLL, letting each application use its own version side by side without conflicting. [Ref. 6]

d. Memory Management

Windows XP memory management is improved in several ways including faster boot and logon, increased pooled memory, and support for larger device drivers. Memory Page Pool has been optimized to handle allocation of the limited physical memory better, reducing extra paging to the disk. And as previously mentioned the paged pool size is twice the Windows 2000 supports. [Ref. 6]

Another improvement is that drivers and kernel components are no longer permitted to allocate memory for “must succeed” requests in low memory conditions. Because of the lack of enough memory for processes, device drivers, and user

applications in low memory conditions, system becomes unstable or even might crash. Now there will be no battle between drivers and processes for memory in low memory conditions. [Ref. 5]

Also in low memory conditions, system processes I/O requests one page at a time using the available resources, instead of parallel processing. This is called I/O throttling and although it decreases performance it prevents the system from crashing. [Ref. 5]

e. Boot Time

Windows XP reduces boot time, by prefetching boot data after the first boot. Unnecessary processes and services are removed from boot sequence allowing faster boot. Also BIOS skips time-consuming diagnostics until after the system boots up successfully [Ref. 5]

f. I/O Subsystem Enhancements

The I/O subsystem of Windows XP provides device drivers to access system resources, manages processes and I/O hardware interaction with user applications.

Microsoft added new APIs to take advantage of the new Windows XP functionality for device drivers. Although Windows 2000 device drivers will work with Windows XP, they must be rewritten to benefit from the new I/O enhancements including the following [Ref. 5]:

- New cancel queue
- File system filter driver routines
- Improved low-memory performance
- I/O throttling
- Direct Memory Access (DMA) improvements
- Web Developing Authoring and Versioning (WebDAV) Redirector
- System Restore
- Volume Snapshot Service (point-in-time copy of a volume)

g. Power Management

In Windows XP Power Manager subsystem is responsible for managing the power usage for the system. Windows XP now implements power management at processor driver level. The new power control standard, ACPI 2.0 is partially implemented. With this new functionality, Windows XP has native support for Intel SpeedStep [Ref. 7] technology, AMD PowerNow [Ref. 8], and Transmeta Long run [Ref. 9] for improved battery life on mobile PCs.

These are not all of the improvements in the kernel. The complete list can be found Microsoft's web site.

The brief and more technical summary of kernel improvements can be seen on Table 2 below.

2. Important Components of Windows XP Architecture

As seen in Figure 1, the Windows XP architecture is comprised of many components. Here I won't explain each of them except the ones strictly or considerably related to security. The most important ones are explained below and some are described in detail in the next section.

a. Kernel Mode and User Mode

One of the most important security, stability and reliability features in modern multi-user and multitasking operating systems is the capability to separate the kernel environment from the users. This is done in Windows XP by using different processor operating modes. Intel X86 and Pentium [Ref. 7] platforms support four level operating modes (also known as rings), but Windows XP uses two of them. These are kernel mode (ring 0) and user mode (ring 3).

Kernel functions	Improvements
Registry	Larger registries, limited only by available system disk space. Improved algorithms for faster queries
Support Enhancements	Cross-session debugging, new quit and detach command for debugging without killing the application, and built-in user mode heap-leak
I/O Subsystem	New input/output (I/O) interfaces for performance enhancement, while retaining compatibility with Windows 2000 drivers. File System Filter driver application programming interface (API) improvements. Support for performance measurements in retail code, and improved low-memory performance
Memory Management	Broad range of improvements, including logical prefetch to improve boot and logon performance, reduced paged pool usage, enhanced terminal server support, support of giant drivers, and Windows XP execution from ROM
Power Management	Native support for processor performance control such including Intel SpeedStep Technology, AMD PowerNow!, and Transmeta LongRun for longer mobile PC battery life. Hibernate, standby, and resume performance have been greatly improved
Improved Boot and Logon Performance	When a Windows XP-based system is first booted, data is saved about all logical disks read operations. On later boots, this information is used to pre-fetch these files in parallel with other boot operations
Headless Support	For 'lights-out' datacenter deployment and remote administration
ccNUMA Support	Provides better performance for Cache Coherent–Non Uniform Memory Architecture (ccNUMA) computers, as well as an interface to let applications tailor their execution characteristics in the ccNUMA environment

Table 2: Kernel improvements for Windows XP (after [Ref. 5])

b. Hardware Abstraction Layer (HAL)

Because Windows XP should be platform dependent, it should work together any kind of hardware seamlessly. Only a small part of the code should be modified to provide this integration. The HAL is the basic element for making this portability possible.

> The HAL is a loadable kernel mode module (Hal.dll) that provides the low-level interface to the hardware platform on which Windows XP is running. It hides hardware-dependent details such as I/O interfaces, interrupt controllers, and multiprocessor communication mechanisms—any functions that are both architecture-specific and machine-dependent. [Ref. 3]
>
> So, rather than access hardware directly, Windows XP internal components, as well as user-written device drivers, maintain portability by calling the HAL routines when they need platform-dependent information. [Ref. 3]

c. Kernel

The Kernel is the heart of Windows XP operating system.

It consists of a set of functions in the Ntoskrnl.exe that provide fundamental mechanisms (such as thread scheduling and synchronization services) used by the executive components, as well as low-level hardware architecture-dependent support (such as interrupt and exception dispatching), that are different on each processor. [Ref. 3] The basic functionalities of Kernel are the following:

- Scheduling thread execution
- Switching context between threads
- Trapping and handling interrupts and exceptions
- Synchronization between processors
- Management of kernel objects

d. Executive

The Windows XP executive is the upper layer of kernel and performs the following types of tasks:

- User mode requests that are exported and callable from user mode.
- Kernel mode requests.

Table 3 lists the major components and support functions of executive, some of which I will describe in detail later.

The support functions are used by the executive components.

Major Components	Description
Configuration manager (registry)	Implements and manages system registry
Process and thread manager	Creates and terminates processes and threads
Security reference monitor (SRM)	Enforces security policies on the local computer. (SRM) will be explained later
I/O manager	Manages device drivers
Plug and Play (PnP) manager	Manages hardware drivers and corresponding memory resources
Power manager	Manages system wide power resources
WDM Windows Management Instrumentation routines	Manages device driver performance and configuration through WMI
Cache Manager	Improves performance by caching data for quick access
Virtual Memory Manager (VMM)	Provides virtual memory that is larger than the physical memory
Support Functions	
Object manager	Handles all the objects and data types that are used by processes, threads, and other objects
Local Procedure Call (LPC) facility	Provides message interaction between processes in local computer
Run-time library	String processing, arithmetic operations, data type conversions, security structure processing
Executive support routines	Includes system memory allocation

Table 3: Windows XP Executive components and functions (after [Ref. 3])

e. Win32 Subsystem

The Win32 subsystem consists of the following three major components that are listed in Table 4.

Win32 Subsytem Components	Description
The environment subsystem process (Csrss.exe)	Support for console (text) windows , and other miscellaneous functions and several natural language support functions
The kernel mode device driver (Win32k.sys)	Contains the window manager and Graphics Device Interface (GDI) that provides graphical usere interface to the user
Subsystem DLLs	Translates Win32 API calls to kernel mode service calls. These DLLs include Kernel32.dll, Advapi32.dll, User32.dll, and Gdi32.dll.

Table 4: Win32 Subsystem components (after [Ref. 3])

In Windows XP, POSIX and OS/2 subsystems are no longer supported. Microsoft removed them from the kernel.

f. Device Drivers

Device drivers are the intermediary system components, usually third party software modules, between the I/O manager and the hardware they are designed for. They are also concern from the security and stability point of view. Because they are a part of kernel they have access to resources that other kernel mode processes can access. In this case, a malicious driver can access the internal system components that are not possible to access from user mode. This means that some third party device drivers, either poorly written or containing malicious intent can cause system wide problems. [Ref. 3]

As stated above Windows XP implements soft-block and hard-block operations against drivers when installing them if they are not digitally signed by Windows Hardware Quality Lab (WHQL).

Device driver do not interact with the hardware themselves, but they use Hardware Abstraction Layer (HAL) to manage them. There are several types of device drivers listed in Table 5.

Device Driver	Description
Hardware device drivers	Manipulate hardware using HAL for input and output operations (includes bus drivers, mass storage drivers)
File system drivers	Translate file I/O requests to device I/O requests
File system filter drivers	Perform operations such as disk mirroring and encryption
Network redirectors and servers	Transmit file system I/O requests to devices and receive such requests
Protocol drivers	Implement a networking protocol such as TCP/IP, NetBEUI, and IPX/SPX.
Kernel streaming filter drivers	Perform signal processing on data streams

Table 5: Windows XP device driver types (after [Ref. 3])

g. System Processes

Processes are the running programs at a given time in Windows XP. They have their allocated memory resources and address spaces. The following system processes appear on every Windows XP system:

- Idle process (for idle CPU time)
- System process
- Session manager (Smss.exe, which is explained below)
- Win32 subsystem (Csrss.exe, which was explained above)
- Logon process (Winlogon.exe, which is explained below)
- Service control manager (Services.exe)
- Local security authentication server (Lsass.exe, which is explained below)
- Svchost.exe (special service containing several groups of services)

These processes are started by the system at boot and are always running. From the security perspective, the most important ones are described here.

h. Session Manager (Smss)

The Session Manager (\Windows\System32\Smss.exe) is the first user mode process that is started in the system. The Session Manager is responsible for managing some specific functions in Windows XP, including the following [Ref. 10]:

- Starting subsystem processes
- Loading necessary DLL files
- Opening additional non-primary paging files
- Initializing system environment variables
- Loading Win32 subsystem (WIN32.SYS and CSRSS.EXE)
- Starting the logon process (WINLOGON)

After starting user mode and logon processes, the *Smss* waits forever for *Csrss* and *Winlogon*. If either of these processes terminates unexpectedly, *Smss* crashes the system.

i. Logon (Winlogon)

The Windows XP logon process (\Windows\System32\Winlogon.exe) is responsible for interactive user logons, logoffs, and secure attention sequence (SAS). Whenever a user initiates the **secure attention sequence** (SAS) keystroke combination, Winlogon starts the logon process. The default SAS on Windows XP is the combination Ctrl+Alt+Delete. SAS is a security precaution for users to be safe from password-capture programs that might imitate the logon process.

The identification and authentication aspects of the logon process are handled by a replaceable DLL named GINA (Graphical Identification and Authentication). The default Windows XP GINA, *Msgina.dll*, provides the default Windows XP logon interface. However, third party developers can provide their own GINA DLL to implement other identification and authentication mechanisms to replace standard Windows XP GINA.

Once the username and password are entered, they are sent to the *local security authentication server (LSASS)* process to be validated. Then *Winlogon* executes the values listed in *Userinit* registry key. The default is to run a process named *Userinit.exe*. Userinit applies the user's settings, starts *Explorer.exe*, and then exits. [Ref. 3]

Winlogon runs silently at the background until SAS is entered or logoff is initiated. Logon process later will be explained in detail.

j. Local Security Authentication Server (LSASS)

The local security authentication server process (\Windows\System32\ Lsass.exe) is responsible for validating the logon credentials that are supplied by *Winlogon.* Lsass uses the appropriate authentication package (Kerberos, NTLM or other packages) to verify the credentials.

> Upon a successful authentication, Lsass generates an access token object that contains the user's security profile and passes it back to Winlogon. Winlogon then uses this access token to create the initial shell process. The shell runs with the user's security context and processes launched from the shell then by default inherit this access token. [Ref. 3]

k. Service Control Manager (SCM)

Services are mostly user mode processes that can be configured to start either automatically at system boot time or manually after the boot. Services normally do not interact with the logged on user and they run in the background throughout the session. The service control manager (SCM) is a system process (\Windows\ System32\Services.exe) that is responsible for controlling these service processes.

From the security perspective services are very important because some of the services are network based (such as IIS or FTP) services. They run with their own security contexts, rights, and permissions and they are independent of the user logged on [Ref. 3]. If compromised they can be used to access system resources.

l. Kernel Objects

The system services, processes and user applications use kernel objects to manage numerous resources, including [Ref. 10]:

- File objects
- Process objects
- Synchronization objects
- IPC and network communication objects

They use the computer resources like other objects and they are accessible only by kernel. However there are several API calls to access the object to access from the user mode.

Kernel objects are protected with a security identifier (SID). Default security setting for objects are creator owners which are given full control. This means that everyone else will be denied access, even an administrator.

C. WINDOWS XP SECURITY ARCHITECTURE

In this section, the architectural basics of security will be mentioned. Later all the aspects of Windows XP security such as logon and authentication, authorization and access control, encrypting file systems, security configuration, user rights, logon rights, and security templates will be studied completely.

1. Security Ratings

The Department of Defense **Trusted Computer System Evaluation Criteria (TCSEC)**, [Ref. 11] published in 1983 , evaluates the commercially available products for specified security features and assurance levels to protect sensitive information. TCSEC contains a range of security ratings, listed in Table 6, that are used to indicate the security features, analysis, and life-cycle management commercial operating systems, network components, and trusted applications should have to achieve defined levels of confidence in security policy enforcement. These security ratings are commonly referred to as "the Orange Book." They extend from a low level to a high level of assurance.

Rating	Description
A1	Verified Design
B3	Security Domains
B2	Structured Protection
B1	Labeled Security Protection
C2	Controlled Access Protection
C1	Discretionary Access Protection (obsolete)
D	Minimal Protection

Table 6: TCSEC Rating Levels

The TCSEC standard consists of trust ratings, where higher levels require more protection and security features to protect data.

Common Criteria (CC) [Ref. 12] was developed in January 1996, with the participation of the United States, United Kingdom, Germany, France, Canada, and the Netherlands for a better product security evaluation specification. Common Criteria is becoming the international standard for product security evaluation.

The Common Criteria specifies 7 of Evaluation Assurance Levels (EALs) for evaluated products. A higher EAL (EAL7) means that the product performs higher level security functions correctly and effectively. The CC is more flexible than the TCSEC trust levels and it is based on the concept of **Protection Profile** (PP), which is a description of security requirements that address threats in a specified environment, to organize security requirements into evaluation levels. It also includes the concept of Security Target (ST) that is an explanation of security requirements of a product.

Windows NT 4 with Service Pack 6a earned a Class C2 rating in both stand-alone and domain configurations [Ref. 12]. Windows 2000, Windows XP and the successors will be rated using the CC rather than the TCSEC because the U.S. government no longer evaluates products against the TCSEC. Microsoft Windows 2000 is currently in the evaluation phase. The first phase was completed in evaluation [Ref. 12].

2. Securing Objects

As with many operating systems Windows XP security model is also based on Security Descriptors (SDs) and Access Control Lists (ACLs). Every object and system resource (files, devices, mailslots, pipes, jobs, processes, threads, events, mutexes, semaphores, shared memory sections, I/O completion ports, LPC ports, waitable timers, access tokens, window stations, desktops, network shares, services, registry keys, and printers) has a security descriptor attached to it when it is created. A security descriptor contains the following information [Ref. 10]:

- The SID of the object owner
- The SID of the primary owning group
- Discretionary Access Control List (DACL)
- System Access Control List (SACL)

3. Security Identifiers (SID)

In Windows XP, accounts are known to the domain controller by their security identifiers (SIDs) rather than their names. A Security Identifier (SID) is a unique value that can vary in length. Domain controller issues an SID for an account when it is created and it remains the same even if the account name is changed. There are some well-known SIDs which are the same in every installation of Windows XP. These SIDs include Administrator, Local Service, Everyone, and Guest. [Ref. 13]

4. Access Control Lists (ACL)

Access Control Lists (ACLs) contain SIDs, permissions, and properties of an object in Windows XP. ACLs can be viewed by opening the Permission and Effective Permission tab of the object properties. There are two types of ACLs [Ref. 13]:

- ***Discretionary Access Control Lists (DACLs)***, which identify the users and groups that are allowed or denied access
- ***System Access Control Lists (SACLs),*** which control how access is audited

5. Tokens

The system uses an object called a **token** (or **access token**) to identify the security context of a process or thread. A security context consists of information that describes the privileges, accounts, and groups associated with the process or thread. During the logon process, Winlogon creates an initial token to represent the user logging on and attaches the token to the user's logon shell process. All programs the user executes inherit a copy of the initial token. [Ref. 3]

Token source	The entity that created the token
Impersonation type	Current impersonation levels
Token type	Primary token (a token that identifies the security context of a process) or an impersonation token (a token threads use to temporarily adopt a different security context, usually of another user)
Authentication ID	Token's creator assigns the token's authentication ID (another kind of LUID) to see whether the token belongs to the same logon session as other tokens the program has examined.
Token ID	Locally unique identifier (LUID) that the SRM assigns to the token when it creates the token
Expiration time	Time period that the token is valid
Primary group	The SID of the primary group
Default DACL	The default DACL that the system uses when the user creates a securable object without specifying security descriptor
User account SID	The SID of the logon account
Group SIDs	SIDs for the groups the account is a member of
Restricted SIDs	An optional list of restricting SIDs
Privileges	List of privileges held by users or user’s groups

Table 7: Tokens (after [Ref. 13])

All tokens are different in size because each account has different privileges. But all tokens might contain the same information as stated in table 7:

The Security Reference Monitor (SRM) compares SID in the token with the SIDs in the object ACLs to determine whether an account can access to that resource.

6. Security System Components

Figure 2 shows the Windows XP security components and how they interact with each other.

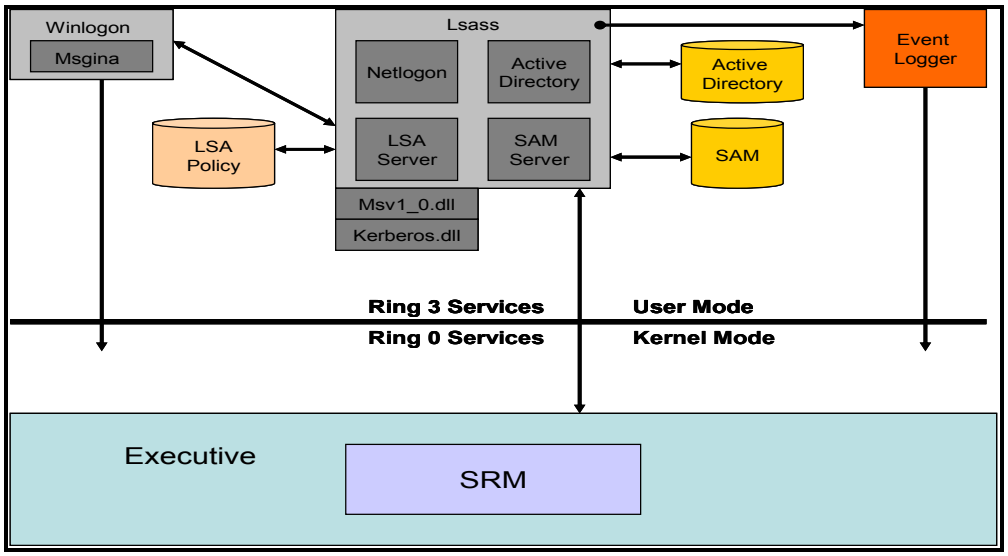

Figure 2: Windows XP security components (after [Ref. 3])

For a better understanding, the most important components are explained in detail below.

a. The Security Reference Monitor (SRM)

The SRM is a component in the Windows XP executive (\Windows\System32\Ntoskrnl.exe) that is responsible for monitoring object access, controlling user rights, and generating security audit messages.

The SRM runs in the kernel mode (actually in the executive in the kernel) and looks at each object's security descriptor (SD) to ensure that object access is consistent with its SD. Here it works with Object Manager.

> The SRM checks security only at the time of handle creation, not at each access, for performance reasons. Because it is less likely that security will change while handle is open. If the access was allowed at the time of handle creation, then access will be allowed until the handle is closed. The algorithm that the SRM uses to determine whether access will be granted is as follows:
>
> - If the object has no DACL, the object is not protected and full access is allowed.

- If the caller has the take ownership name privilege, the SRM immediately grants the caller the right to modify the owner field in the SD before further examining DACL.
- If the caller is the owner of the object, the caller is granted read-control and write-control (the ability to view and modify DACL) on the DACL before further evaluating DACL.
- Each ACE (Access Control Entries) in the DACL is examined in order. If the SID in the ACE matches an enabled SID in the token (primary or impersonation), the ACE is processed.
- If all of the access rights the caller requested can be granted, the object access succeeds. If any of the requested access rights can't be granted, the object fails. [Ref. 10]

The SRM also evaluates the SACL in the same way and writes audit events to the event log if necessary.

b. The Local Security Authority (LSA)

Local security authority subsystem is a privileged user mode process (\Windows\System32\Lsass.exe) that enforces local system security policy (such as logon, password and audit policies, privileges granted to users and groups, and the system security auditing settings). It is also responsible for many other security related tasks such as user authentication, and sending security audit messages to the Event Log.

> The SRM, which runs in kernel mode, and Lsass, which runs in user mode, communicate using the LPC facility. During system initialization, the SRM creates a port to which Lsass connects. When the Lsass process starts, it creates an LPC port. The SRM connects to this port, resulting in the creation of private communication ports. The SRM creates a shared memory section for messages. Once the SRM and Lsass connect to each other during system initialization, they no longer listen on their respective connect ports. Therefore, a later user process has no way to connect successfully to either of these ports for malicious purposes—the connect request will never complete. [Ref. 3]

Figure 3 shows the communication between LSA and SRM.

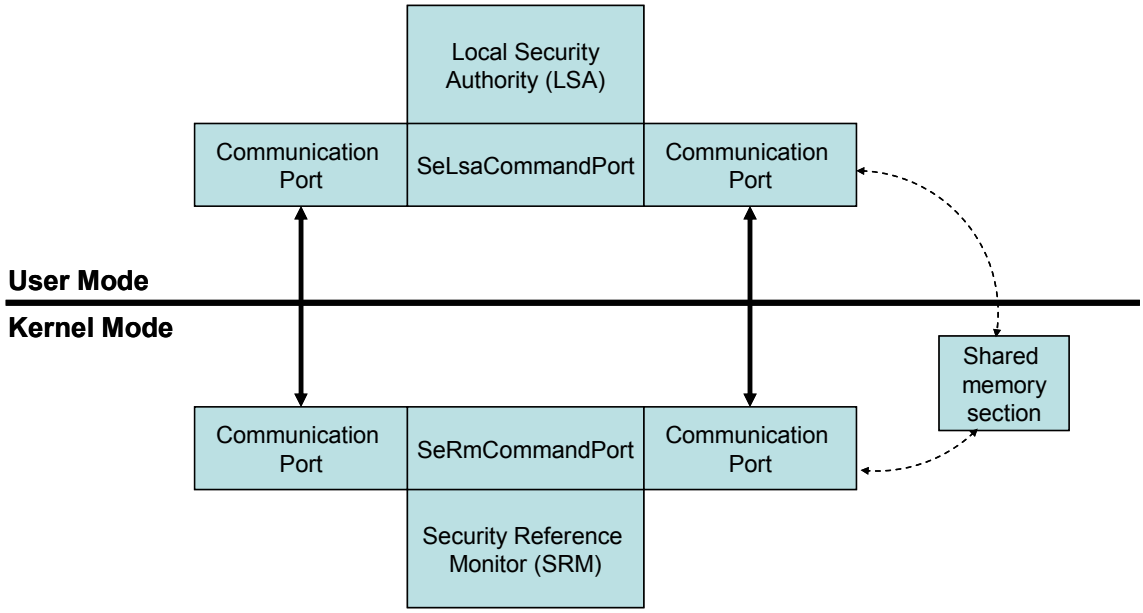

Figure 3: Communication between the SRM and LSA (after [Ref. 3])

> ***Lsass policy database*** is the database that contains the local system security policy settings. It includes such information as what domains are entrusted to authenticate logon attempts, who has permission to access the system and how (interactive, network, and service logons), who is assigned which privileges, and what kind of security auditing is to be performed. The Lsass policy database also stores "secrets" that include logon information used for cached domain logons and Win32 service user-account logons. [Ref. 3]

Security Accounts Manager (SAM) service is a group of processes responsible for managing the SAM database that contains Local account and policy information.

SAM database is the database that contains the local account and policy information (local users and groups and their passwords and other attributes).

Active Directory is the directory service that contains information about objects in a domain. Active Directory stores all the information about the objects such as users, groups, and computers and their respective passwords and privileges.

Logon process (Winlogon) is a privileged user mode process (Windows\System32\Winlogon.exe) that is responsible for responding to the SAS and for interactive logon as explained earlier.

Graphical Identification and Authentication (GINA) is a replaceable DLL that contains user's credentials and runs in the Winlogon process. The standard GINA is Msgina (\Windows\ System32\Msgina.dll) in Windows XP.

Net Logon service (Netlogon) is a Win32 (user mode) service (\Windows\ System32\ Netlogon.dll) that runs inside Lsass and handles network logon requests in domains.

D. WINDOWS XP SECURITY FEATURES

The changed security-related features in Windows XP Professional are summarized in Table 8. New features are summarized in the table 9 below.

Security Feature	**Description**
Everyone membership	The built-in Everyone group no longer includes members of the Anonymous group.
Simple sharing	By default, systems that are not connected to a domain, all attempts to log on from across the network will be forced to use the Guest account.
Administrative ownership	All resources such as files and folders that are created by a member of the Administrators group by default belong to the individual who creates them.
Encrypting File System (EFS) recovery agent	Attempting to configure an EFS recovery policy with no recovery agent certificates enables users to encrypt files without a Data Recovery Agent (DRA).
Permissions for installing printers	In order to install a local printer users must belong to the Power Users or Administrators group and have the Load/Unload Device Driver privilege.
Blank password restriction	To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console.

Table 8: Changed security features in Windows XP (from [Ref. 14])

Some security features are only for non-domain environments. These features can only be applied to standalone computers. Others can be applied to workstations that are part of a domain. Most of the features can be configured by Group Policy settings in the domain controller server. But some of them can be configured both by Local Security Settings Snap-In in the workstation and by Group Policy in the domain controller. In this case, Group Policy objects that are applied via domain take precedence over local

security policies and prevent the local settings to be changed. Windows XP has a new tool to see the effective security settings in the local computer: the Resultant Set of Policy (RSoP) MMC snap-in. [Ref. 13]. This feature will be explained later.

Security Feature	**Description**
Corporate Security	Group Policy objects
Encrypting File System	Sharing encrypted files (network file shares and Web Distributed Authoring and Versioning (WebDAV) Web folders)
	Disabling data recovery agents
	Group Policy and command line management
Certificate Services	Multiple levels of a CA hierarchy
	Cross-certified trust network
Credential Management	Credential prompting UI
	Stored user names and passwords
	Keyring (manually managing the stored credentials)
	Password Reset Wizard
	New service accounts (LocalService and NetworkService)
Fast User Switching(non-domain systems)	Switching from one user account to another without closing applications or logging off
Personal Privacy	Cookie management
Internet Connection Sharing(ICS)	One computer, connects directly to the Internet and shares its connection with the rest of the computers on the network
	Location-aware group policy
Internet Connection Firewall	Active packet filtering (ports on the firewall are dynamically opened only for as long as needed to enable to access the desired services)
	Location-aware group policy
	Stateful packet filter
Software Restriction Policies	Preventing unwanted applications from running
Internet Protocol Security (IPSec)	Encrypting data before transmission
	Data hashing
	Authentication
	Blocking ports and protocols
Smart Card Support	Integrated circuit card (ICC) for storing certificates and private keys
	Tamper-resistant storage
	Isolating critical security computations
	Mobility
Kerberos	Secure and efficient authentication
Stored User Names and Passwords	Different credentials for different resources.

Table 9: New security features in Windows XP (after [Ref. 14])

It is easier to understand Windows XP security, if we analyze them in three areas:

- Logon and Authentication
- Authorization and Access Control
- Network Security

In the table 10 we can see the security areas and their related security features.

Security Area	**Security Features**
Logon and Authentication	Security Groups
	Security Policies (account policy, local policies, audit policies, user rights assignment, public key policies, Kerberos policy and IP Security policies)
Authorization and Access Control	File and Folder Permissions (File
	Encrypting File System (EFS)
Network Security	Internet Connection Firewall (ICF)
	TCP/IP Filtering
	Smart Cards
	Extensible Authentication Protocol
	Wireless Security (802.1x)

Table 10: Security areas

1. Logon and Authentication

Authentication and logon processes, and the services that take part in these processes have been explained previously in this chapter. In this section, the security features related to authentication and logon will be explained briefly.

a. Security Groups

By organizing accounts into groups, administrators can easily manage account permissions including access to folders and files or access to system wide settings. Using security groups, administrators can assign the same security permissions to all users in a group. This provides effective security permission assignment across all members of a group.

Groups and users are contained in the Security Accounts Database for domains. Security Groups can be described in two ways [Ref. 13]:

- according to their scope (such as Global or Universal)
- according to their purpose, rights, and role (such as the Everyone, Administrators, Power Users, or Users groups)

There are several built-in groups in Windows XP that define the access levels for accounts on file system, system services, and other local and network resources: Administrators, Power Users, and Users.

b. Security Policies

An administrator can implement most of the security settings by using the Local Security Policy for computers not connected to a domain or by the Group Policy for computers connected to a domain. In Group Policy, many security related settings can be modified, including ACLs for file systems, registry and services.

Account Policies: These policies include password settings, account lockout settings, and Kerberos settings (for the domain controller). They are used to control security settings for group and user accounts.

For domain-wide account policies Group Policy is used. Default Group Policy object is applied by domain controller to set the account policies for domain accounts. These settings are applied to all domain accounts regardless of the organizational unit in which domain resides. Thus, although there are different local account policies in the different organizational units, there is only one account policy for the accounts in a domain. Windows XP comes with a new Group Policy object that can be applied throughout a Windows 2000 domain. [Ref. 13]

Within ***Password Policy***, these settings can be controlled:

- Minimum and maximum password age
- Enforcing password history
- Minimum password length
- Complexity requirements

Account Lockout Policy is used to disable accounts after a specified number of unsuccessful logon attempts. The account is locked for a specified time if this

policy is enabled after the failed logon attempts reach the specified number. These options can help the administrators to detect and block attempts to break passwords.

Account Lockout Policy lets administrators to define three settings:

- ***Account lockout threshold*** determines the number of failed logon attempts after which user's account will be locked.
- ***Account lockout duration*** determines the number of minutes that the account will be locked.
- ***Reset account lockout counter after*** determines how many minutes must elapse until the count will be reset after a failed logon attempt.

Local Policies: These policies include auditing policy, assignment of user rights and privileges, and various security options that can be configured locally on a particular Windows XP based computer.

Audit Policies include operating system events and account activities such as successful and failed logon attempts that may be logged by Event Viewer. Each of these entries may be set for logging success, failure, or no logging.

User Rights Assignment contains entries for privileges that may be assigned to users or groups. These settings are used to allow or deny users to access the computer resources.

Security Options include settings for accounts, auditing, devices, domain controllers, domain members, interactive logon, network client, network server, network access, network security, recovery console, shutdown, system cryptography, and system objects. This grouping is new in Windows XP and it is very useful to manage settings easily. These settings are a broad range of security settings that are defined and applied by Group Policy in domain environments.

Event Log Settings: This is used to configure auditing for security events such as successful and failed logon and logoff attempts.

Public Key Policies: These policies contain settings for user and computer certificates. These settings include auto enrollment and renewal of certificates.

Software Restriction Policies: This is a new kind of policy feature in Windows XP that allows administrators to prevent unwanted applications, such as viruses or other harmful software, from running. This is done by classifying applications as trusted or untrusted. After trusted and untrusted applications have been identified, software restriction policy is applied to control each application's ability to run.

Software Restriction Policies includes two key items [Ref. 13]:

- ***Security Levels***, which define the default authorization level at which a user is allowed to run a piece of software.
- ***Additional Rules***, which specify the maximum authorization level at which a piece of software is allowed to run on that computer.

When a user attempts to run a software application, the computer uses the maximum values of these two components to determine the authorization level at which the application is allowed to run.

This policy can apply to an entire computer or to individual users by using Domain Security Policy in domain controller.

There are two Security Levels, **Unrestricted** and **Disallowed**. Unrestricted settings are used to define the programs that are allowed to run as long as users have permissions for those programs. Unless explicitly allowed by additional rules, **Disallowed** is used to specify the programs that are forbidden to run.

Security Level rules are defined according to the following criteria associated with that program:

- ***Path*****:** An application is allowed or disallowed by creating a rule based on the application's file path in the computer.
- ***Hash*****:** An application is allowed or disallowed based on the application's computed hash value. Hash value is cryptographic calculation derived from the contents of the file. Moving or renaming the file does not prevent this rule to be applied.

- ***Certificate:*** An application is allowed or disallowed based on the certificate signed for that program. Moving or renaming the file does not prevent this rule to be applied.
- ***Internet Zone:*** An application is allowed or disallowed based on the Internet zone (specified by Internet Explorer) from which the application is downloaded. These rules apply only to Windows Installer packages.

Additional Rules allow administrators additional control over Software Restriction Policies:

- ***Enforcement Properties*****:** These rules are used to exclude or include software library files.
- ***Designated File Types*****:** This is a list of file types that are considered to be executable codes such as Visual Basic Scripts. This list can be modified by adding or removing file types.
- ***Trusted Publishers*****:** This rule defines the users that are allowed to select trusted publishers.

IP Security Policy: IPSec is an emerging standard for securing data and communication over a public network. In Windows based networks IPSec protects the contents of the IP packets and defends the network against attacks by using packet filtering. It provides strong protection using cryptography-based protection services, security protocols, and dynamic key management. In Windows XP it uses DES (Data Encryption Standard) and 3DES (Triple DES). IPSec packets use two protocols:

- ***IP Protocol 50:*** Encapsulating Security Payload (ESP) format defining privacy, authenticity, and integrity.
- ***IP Protocol 51:*** Authentication Header (AH) format defining authenticity and integrity. It does not define privacy.

Authentication may be provided by Kerberos, certificates provided by a CA. During authentication, keys are exchanged and integrity and encryption are negotiated using Internet Key Exchange (IKE) on UDP port

> 500. Integrity is assured by using Authentication Header (AH). AH wraps the IP packet in an IP Protocol 51 packet, which includes either an SHA1 or MD5 checksum of the original packet, which the end station may use to verify that the packet was not modified. Integrity and Encryption may be combined using Encapsulating Security Payload (ESP).With ESP, the original packet is encrypted using the previously negotiated key, then the checksum is calculated on the encrypted packet using SHA1, then the encrypted packet is placed in the IP Protocol 50 packet and sent to the destination. [Ref. 15]

IPSec policies are configured by using Group Policy snap-in in domain controller. Three preconfigured IPSec policies are defined by default installation: Client (respond only), Server (request security), and Secure Server (require security). After choosing one of these three rules, IP Filter lists and actions can be created for the rule.

Restricted Group Policy: This policy is used to manage the members of built-in restricted group. These groups include built-in groups such as Administrators, Power Users, Print Operators, Server Operators, and domain Administrators. Groups can be added to the Restricted Groups list or removed from the list by this policy.

System Services: These settings include security settings for services such as network services and third-party services. Service startup mode (automatic, manual, or disabled) can be configured by this policy. Services are important because they have the ability to access both local and domain objects. This ability poses some risks if they are compromised. These considerations will be discussed later in analysis section.

Registry: This policy includes settings for security descriptors on registry keys and subkeys.

File System: This policy includes settings for local file system. These settings contain file or directory paths and security descriptors for each file.

c. Security Templates

Windows XP Professional provides predefined security templates to apply security settings throughout the domain. By using these templates it is easy to create security policies for different organizational needs. They are easily customized by using the Security Templates snap-in and can be used to configure domain computers by importing them into the Group Policy in the domain controller. If Windows XP is used in

Windows 2000 server based domains, it will be better to use the templates that come with Windows XP. Because these are the latest templates and they include new security settings.

A security template can also be imported in Security Configuration and Analysis snap-in for analyzing system security violations.

The security templates are stored in the *Systemroot*\Security\Templates folder by default. The predefined templates are:

- Setup Security (Setup Security.inf)
- Compatible (Compatws.inf)
- Secure (Secure*.inf)
- High Secure (Hisec*.inf)
- Root Directory Permissions (Rootsec.inf)

These templates are meant to be applied incrementally.

Setup Security (Setup security.inf): Setup security is the baseline template containing the default security settings applied during clean installation of Windows XP.

Compatible (Compatws.inf): This template contains default permissions for three local groups: Administrators, Power Users, and Users. Administrators have the most privileges, while Users have the least.

It loosens the default permissions for the Users group so that older applications can run under these settings. Power Users group members are removed in the Compatible template to prevent the users running non-certified applications. [Ref. 13]

Secure (Secure*.inf): The Secure configuration includes increased security settings for Account Policy, Auditing, and some common security-related registry subkeys and entries. File, folder and registry object settings are not implemented by this template. Those settings were already implemented secure enough by default.

> The Secure templates also provide further restrictions by preventing anonymous users (for example, users from untrusted domains) from [Ref. 13]:

- Enumerating account names and shares
- Performing SID to name or name to SID translations

High Secure (Hisec*.inf): The High Secure template sets security settings for network communications and imposes further restrictions on network traffic and protocols used between clients and servers. This template ensures that all network communications are digitally signed and encrypted by default encryption package. All of the computers configured with highly secure settings can only communicate with other machines running Windows NT 4.0 Service Pack 4 or higher.

Root Directory Permissions (Rootsec.inf): This is a new template that specifies the new permissions for the root of the system drive. This template can be used to reset the default root directory permissions. When applied it propagates the permissions on all subfolders and files.

d. Resultant Set of Policy (RSoP)

> The Resultant Set of Policy (RSoP) snap-in (Rsop.msc) enables administrators to poll and evaluate the cumulative effect that local, site, domain, and organizational unit Group Policy objects (GPOs) have on computers and users. [Ref. 13]

With this tool it is easy to see the settings in local computer that is a part of a domain. This tool can be used locally or remotely. When the computer is a member of more than one domain, then there are different settings that apply to that computer. To see the effective settings RSoP can be used.

e. Kerberos Version 5 Authentication Protocol

In Windows XP authentication can be provided using several protocols:

- Kerberos V5 protocol
- NTLM protocol

Kerberos protocol is the default protocol to be used in Windows XP, if domain controllers and client computers are running Windows XP or Windows 2000 in the domain. Otherwise NTLM protocol will be used to authenticate domain accounts.

> The Kerberos version V5 protocol uses secret key encryption to protect logon credentials that travel across the network. The same key can then be

used to decrypt these credentials on the receiving end. This decryption and the subsequent steps are performed by the Kerberos Key Distribution Center, which runs on every domain controller as part of Active Directory. [Ref. 13]

2. Authorization and Access Control

Windows XP includes a number of features that can be used to protect selected files, applications, and other resources from unauthorized use. These features include:

- Access control lists (ACL)
- Security groups
- Group Policy

The access control models have these key concepts and characteristics [Ref. 13]:

Discretionary access to securable objects: In Windows XP the creator owner of an object has ultimate control over that object. In previous versions of Windows in addition to creator owner, Administrator has also full control. Creator owner can give specific permissions such as "Write", "Read", and "Delete" to any user or groups, or deny access to that object completely.

Inheritance of permissions: In NTFS file system, the permissions of a folder can be inherited by the subfolders and files which it contains. Also new objects can be set to inherit the permissions from the folder that it resides as well.

Auditing of system events: Auditing feature can be used to log accesses to objects or changes in object permissions, even if another administrator makes that change. In Windows 2000 based domains auditing settings are configured by Group Policy in domain controllers.

a. NTFS

NTFS includes features such as advanced file system security, recovery from failures, support for large volumes, and support for long names. The NTFS file system provides the capability to manage authorization and access control on file and folder permissions and auditing in very granular ways. It also allows for encrypting files via the EFS. [Ref. 15]

b. Encrypting File System

The Encrypting File System (EFS) helps to store sensitive data securely by encrypting them. This offers an additional layer of protection so that sensitive data is secure. Encrypted files are accessible only by the user who has encrypted them and cannot be opened even by an Administrator unless he is a designated recovery agent.

Files or folders must be in NTFS volumes in order to be encrypted, FAT and FAT32 file systems do not support EFS. Although encrypted files are secure in local system, they are transmitted in plain text over the network. In this case they can be captured by network sniffers while being transmitted. To eliminate this risk EFS can be used with Web Folders that can transmit data encrypted by using Web Distributed Authoring and Versioning (WebDAV) protocol. [Ref. 15]

> Although the encrypting and decrypting of files is mostly transparent to users, it is fairly complex process. Each file has a unique randomly generated file encryption key created, which is used to encrypt the file and is needed to decrypt the file's data later. The file encryption key is then encrypted by user's public key, and the public key of each of recovery agents also encrypts the file encryption key. (There are now at least two keys available to decrypt the file with). To decrypt a file, the file encryption key has to be decrypted first. User, who encrypted the file encryption key with his private key, decrypts the file encryption key that is used to decrypt the original file. Alternatively, the designated recovery agents can also decrypt the file encryption key by using their own private key and thereby recover the encrypted file. [Ref. 15]

3. Network Security

Windows XP has several features to provide network access security. The Internet Connection Firewall and TCP/IP Filtering are used for securing network communications by blocking unwanted incoming traffic. Smart cards are another way of user authentication for domains.

a. Internet Connection Firewall (ICF)

ICF is a basic firewall that protects a computer that is connected directly to the Internet via dial-in, cable modem, DSL, satellite, or other means. It is limited in its capabilities and for advanced network security control a commercial firewall can be used.

It is disabled by default and must be configured and enabled for each Internet connection. Its essential function is to make the computer invisible to outside world or Internet. It monitors the incoming traffic filtering unsolicited packets from Internet. It is a stateful firewall keeping a table for all Internet access originating from computer. After that it examines incoming packets, and allows the ones that are only part of a session originating from the computer. This means that a packet arriving at the computer is checked against the table to see if there is a request for that packet sent earlier. If so it is allowed, if not it is dropped and logged.

By default all unsolicited inbound packets will be dropped. But user can configure the ICF to allow traffic for specified services. These are FTP, IMAP (Internet Mail Access Protocol version 3, and 4), SMTP (Internet Mail Server), POP3 (Post Office Protocol version 3), Remote Desktop, HTTPS (Secure Web Server), Telnet Server, and HTTP (Web Server). Also all incoming ICMP echo (ping) packets will be blocked. But it can be configured to be allowed by ICF. ICF can log certain types of events such as dropped packets and successful outbound connections. By default there is no logging.

This firewall is intended to use in home and small office networks. Today broadband connections such as DSL and cable modem are widespread. These are "always-on" connections increasing the exposure to malicious attacks. ICF can be a good step to protect broadband connections for home and small office networks.

It is not recommended for local LANs because ICF blocks file and printer sharing.

b. TCP/IP Filtering

TCP/IP filtering can provide a measure of security for a Windows XP system by controlling ports and incoming data types. However, in terms of the degree of protection it is not as effective as ICF or commercial firewalls.

TCP/IP filtering can be applied for domain environments by Group Policy very effectively. Administrators should create IPSec policies that meet the organizational needs.

c. Biometric and Smart Cards

Smart cards are credit card–sized integrated circuit cards that contain a microprocessor, RAM, and ROM (EEPROM) that can be used to store digital certificates or private keys. Smart card readers are used by computers to access data on smart cards securely. It uses a PIN instead of passwords. Smart card readers attach to computers using peripheral interfaces such as RS-232, PC Card, and Universal Serial Bus (USB). Smart cards are used for only domain accounts [Ref. 15]

Now Windows XP support biometric devices such as fingerprint or iris scanners. These devices can be integrated into a domain authentication process.

d. Extensible Authentication Protocol (EAP)

EAP is an extension protocol to the Point-to-Point Protocol (PPP) which is defined in RFC 1661 [Ref. 16]. EAP is defined in RFC 2284[Ref. 17]. EAP does not require authentication but provides optional authentication phase. [Ref. 15]

Windows XP supports two EAP types that are defined in RFC 2284: EAP-MD5 and EAP-TLS:

EAP-MD5 is a simple account authentication method that uses the same challenge-handshake protocol that is used by the Challenge Handshake Authentication Protocol (CHAP). EAP-MD5 does not support encryption.

EAP-TLS is a Secure Channel (SChannel) authentication and encryption protocol in which the client and the server must prove their identities mutually. It provides integrity-protected cipher-suite negotiation and key exchange between clients and servers by using public key cryptography (PKI). [Ref. 15]

e. Wireless Network Security (802.1x Authentication)

Windows XP supports IEEE 802.1x authenticated network access for both Ethernet and wireless 802.11 networks. IEEE 802.1x is a port-based access control that provides authentication for network resources, by requiring account identification, centralized authentication, and dynamic key management. [Ref. 15]

> When users attempt to connect to the network, the switch or access point sends an EAP authentication request. Depending upon the 802.1x configuration of the Windows XP network adapter, Windows XP prompts

> the user (via a balloon above the system tray icon for the network adapter) to click to authenticate. Windows XP then prompts the user for either a username and password or her smart card. The authentication information is passed back to the switch or access point and then is relayed from the switch or access point to the RADIUS server. The RADIUS server then evaluates the request, verifies that the user is allowed access, and passes its approval for access and possible optional information for the switch, such as VLAN membership or 802.11 encryption keys. The switch or access point may be configured to reauthenticate periodically or to generate new encryption keys periodically. [Ref. 15]

f. Automatic Updates

With automatic updates Windows XP downloads and installs updates whenever they are available. Because most updates are security related, by enabling automatic updates the computers will be safer than the ones that are not patched.

Automatic updates can be configured by Group Policy. There are three options: It can be set not to download at all or to download but not to install them. The user may then install them at a convenient time. The last option is to download and install all updates automatically.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EXPERIMENTAL SETUP

A. INTRODUCTION

Windows XP was built over the Windows 2000 Operating system. Many security features remain the same, but there are also new features that are introduced for the first time. Some of them are stand-alone computer-specific, and some are built for domain environments. For the context of this thesis, the main focus will be on domain-specific security features. In the following sections, the actual network setup and domain security configuration will be analyzed along with security templates.

B. EXPERIMENTAL SETUP

In order to analyze Windows XP security, we simulated a network using three computers. One computer ran Windows 2000 Server; the others ran Windows XP Professional and Windows 2000 Professional operating systems.

The server is the domain controller of the XP domain. The domain is an Active Directory based domain. The server is also a DHCP and DNS server for the domain. The configuration can be seen in Figure 4 below.

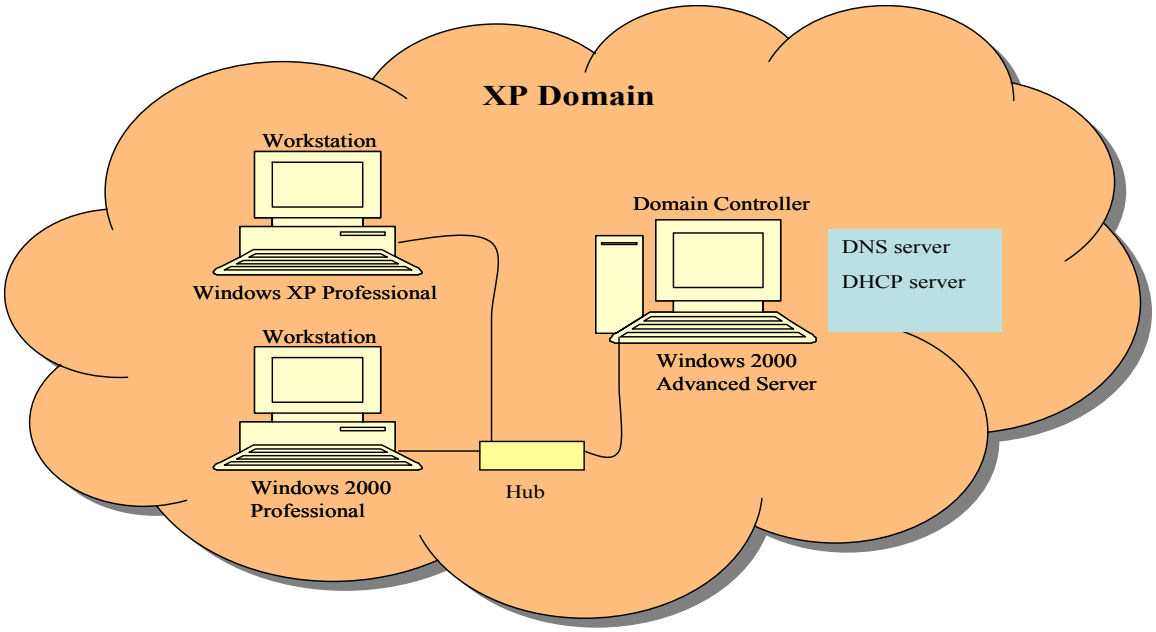

Figure 4: Experimental domain

The hardware specifications of the computers are summarized in Table 11 below.

Hardware specifications	Windows 2000 Advanced Server	Windows XP Professional	Windows 2000 Professional
Processor	Intel Pentium III 784 MHz	Intel Pentium III 784 MHz	Intel Pentium 4 1400 MHz
Mainboard	Intel D815EEA	Intel D815EEA	Dell 1D0V01
BIOS	Intel EA81510A	Intel EA81510A	Phoenix 1.10 A08
Video adapter	32 MB NVIDIA RIVA TNT2 Pro	32 MB NVIDIA RIVA TNT2 Pro	32 MB DDR NVIDIA GeForce2 GTS
Hard Drives	7 GB IBM-DPTA-371360	7 GB IBM-DPTA-371360	18.61 GB SCSI Hard Disk
Storage Devices	IDE-CD R/RW 8x4x32	IDE-CD R/RW 8x4x32	CD-ROM / DVD Drive
Network Adapters	2 3Com EtherLink 10/100	3Com EtherLink 10/100	3Com 3C920 Integrated
Multimedia Devices	Creative Audio PCI	Creative Audio PCI	SoundMAX Integrated Digital Audio
Memory	256 MB SDRAM	256 MB SDRAM	256 MB SDRAM

Table 11: Hardware specifications of the computers

C. TOOLS

Because there were so many security-related features to look at, I decided to focus on the security templates and security settings in this analysis. The new policy settings, what we can configure with them, and the impact on the overall security are analyzed in the following sections.

After the new policy settings, templates, and features were analyzed, I used network security scanners to scan Windows XP with some well-known scanners: demo version of Retina [Ref. 18], Languard [Ref. 19], and Microsoft's Baseline Security Analyzer [Ref. 20].

Retina: Retina is a well-known and highly acclaimed network security scanner. In our scans it scanned the computer much faster than the other scanners.

It is easy to use and updates its vulnerability database frequently. It uses a kind of artificial intelligence technology called Common Hacker Attack Methods (CHAM) to

scan known and unknown vulnerabilities. Retina checks these features for vulnerabilities [Ref. 18]:

- Accounts with details such as password history, cached logons, password vulnerabilities, and accounts with no passwords.
- NetBIOS and NetBIOS enumeration
- HTTP
- CGI and WinCGI Scripting vulnerabilities
- FTP
- DNS
- DoS vulnerabilities
- POP3
- SMTP
- LDAP
- TCP/IP and UDP
- Registry
- Services
- Users with account details

Since we used demo version, its capabilities are limited; it scans one computer at a time and does not allow for the generated report to be saved. But as we will scan only one computer and use only some of its features, Retina serves its purpose.

Languard: Languard is another intrusion detection scanner tool that generates results comparable to Retina which costs much more than Languard. The results can be saved as an HTML file so that it can be customized and queried [Ref. 19]. It can check almost as many features as Retina for potential vulnerabilities [Ref. 19]:

- Service pack levels of target machines

- Security patches applied and not applied
- Shares including administrator shares
- Open ports
- User and group accounts with password policy details such as last logon and password age
- Auditing policy
- Potential Trojans installed on users' workstations with its regularly updated Trojan database
- NetBIOS names
- Running services
- Network devices (e.g. NIC cards) with details
- Key computer information in registry

At the end of its report Languard lists the alerts with vulnerability descriptions.

Microsoft Baseline Security Analyzer (MBSA): Microsoft has introduced a new security analyzer for common security vulnerabilities and misconfigurations. MBSA scans operating system for [Ref. 20]:

- Missing updates, patches, and hot fixes
- Accounts and password policies
- Guest account status
- Auditing policy
- Unnecessary services
- File system status
- Shares
- Internet Explorer security zone

Like Languard MBSA creates an HTML report to view the results. The results are divided in sections and can be viewed both in browser and in MBSA's graphical user interface.

D. METHODOLOGY

In our analysis and vulnerability scans, I will focus on the new security policy settings and vulnerabilities that can be avoided by configuring related security settings appropriately. The new security settings that can be applied through security policies will be described in detail including their default settings.

Some of the results of vulnerability scans are directly related to the settings in the security template that are applied. These include account settings, network access settings, file security settings, and registry settings. In the vulnerability scans we will focus on open ports and default services.

After the analysis is done a recommended security template will be created using the results of analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SECURITY ANALYSIS

A. INTRODUCTION

In this chapter, we assess Windows XP security. There are some major improvements in Security Policy settings and other security configuration settings in Windows XP. We will look at these changes in this chapter.

B. SECURITY POLICIES AND TEMPLATES

There are many security settings to be configured in the domain level. For workstations, these settings can be applied using the Security Configuration Tool-set in domain controller. This tool-set is an easy way to apply and control the security settings in a Windows 2000 based domain. Domains, which implement an "Active Directory" domain structure, can configure and apply additional security configuration options, such as a Kerberos policy for clients running Windows 2000 Professional and Windows XP Professional. These additional settings are not available in security templates. But, the Security Configuration Tool-set in domain controllers configures them. Note that some of the settings in the templates that come with Windows XP are not applicable to Windows 2000 workstations and are just ignored in Windows 2000 computers. Detailed information about templates can be found in Chapter 2.

In our experimental domain, we implemented the Active Directory structure for the domain. We configured Domain Security Policies with workstation security templates that come with Windows XP. They were applied incrementally and scanned by vulnerability scanners such as Retina (demo version from eEye Company), Languard scanner and Microsoft's Baseline Security Analyzer. We looked at default services, open ports and other possible security risks in this analysis.

1. New Security Settings in Windows XP Templates

With new features and security improvements, the settings that can be applied by templates and Security Configuration Tools have significantly increased. More granular settings can be applied by using these templates instead of Windows 2000 templates. Some of the features that were applied manually now can be applied easily with these

settings. The new security settings implemented in Windows XP are shaded in a template comparison table in Appendix C. Some of the important changes are discussed below.

a. Logon and Authentication Settings

Security Policy easily configures strong security settings, for password and authentication.

Sharing and security model for local accounts: This setting determines the authentication behaviors of network logons that use local accounts. There are two choices that can be set; **Classic** and **Guest only**. If this setting is set to **Classic**, network logons authenticate as local accounts. If this setting is set to **Guest only**, network logons authenticate as Guest account. By using Classic model access control over network resources will be controlled explicitly because there are different user account permissions. By using the Guest only model, all users will have the same access permissions over network resources because they will have only Guest privileges, which can be either Read Only or Modify [Ref. 13]. **Guest only** is the default model for Windows XP. This policy does not apply to computers in a domain.

By default, members of the Guests group do not have the access permissions on the application and system event logs. For other resources they have the same privileges as members of the Users group. Thus anybody can log on to workstations with limited Guest privileges without having an account in that computer or domain. [Ref. 13]

Attackers could gain access to computers by use of the Guest account. Since the Guest account and Guests group pose security risks and are not used in domain environments, these accounts should be locked out by using the "Active Directory Users and Computers" tool in the domain controller. Disabling the Guest account might not be enough.

Limit local account use of blank passwords to console logon only: In Windows XP, accounts without passwords are limited to logon only locally at the physical computer. They cannot logon to local computers using remote connections.

This setting determines whether an account without a password can log on to local computer by using remote connections such as Terminal Services, Telnet, and FTP. If this setting is enabled, a local account with blank password cannot connect to local computer from a remote client. This setting is **enabled** by default.

This setting does not affect the domain logons that are performed from a local computer in the domain.

Do not store LAN Manager hash value on next password change: The LAN Manager stores the LM hashes of passwords in the SAM. This setting prevents LAN Manager from storing LM hashes in the SAM. If enabled, the new setting takes effect at the next password change for new password. This setting is set to **none** by default.

Because the LM hashing technique is not strong, passwords can be easily cracked by password cracking programs such as L0phtcrack [Ref. 21]. Enabling this setting, removes the LM hash completely. Another way of achieving strong password security for individual accounts is to create a strong password such as more than 12 characters.

Minimum session security for NTLM SSP based (including secure RPC) clients and servers: These settings are used to control application-to-application communication security settings between clients and servers by requiring encryption standards.

Windows NT supports two different standards of challenge/response authentication for network logons:

- LAN Manager (LM) challenge/response
- NTLM version 1 challenge/response

Windows XP supports both of them and NTLM version 2. LM is the least secure one and allows interoperability with the previous Windows operating systems. NTLM provides improved security for connections between clients and servers. There are some options that can be chosen. Administrators can configure this setting by choosing all or none of the following:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128 bit encryption.

By default there are no requirements.

The settings described above were also available in previous versions of Windows, but they are now easily configured via the Security Policy. Requiring NTLMv2 for authentications in Windows XP will prevent SMB capture programs from capturing LM hashes. [Ref. 22]

These settings must be used along with "LAN Manager Authentication level" setting that determines which challenge/response authentication protocol is used for network logons. This setting is **undefined** by default. The authentication levels used by clients and accepted by servers are as follows [Ref. 13]:

- **Send LM & NTLM responses:** Clients use LM and NTLM authentication and never use NTLMv2 session security; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send LM & NTLM - use NTLMv2 session security if negotiated:** Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send NTLM response only:** Clients use NTLM authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.
- **Send NTLMv2 response only:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.

- **Send NTLMv2 response only\refuse LM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).
- **Send NTLMv2 response only\refuse LM & NTLM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).

For the server, this setting is defined for the least secure level (Send LM & NTLM responses).

These settings are important especially when Windows XP is deployed on mixed networks (networks that contain operating systems prior to Windows 2000, such as Windows 98). Since these three settings are not defined by default, it might be possible to sniff the SMB credentials and crack them by using third party tools such as SMBCapture [Ref. 21] and L0phtcrack [Ref. 21].

If the network contains only Windows 2000 and Windows XP workstations Kerberos authentication should be used instead of NTLM. In addition, as the client server communication is digitally signed (when possible) by default, it ensures that integrity and authenticity of SMB messages.

Do not allow Stored User Names and Passwords to save passwords or credentials for domain authentication: This setting determines whether the Stored User Names and Passwords functionality saves account credentials in user's profile for future use. If this setting is enabled, it prevents the Stored User Names and Passwords from storing account credentials. This setting is **disabled** by default.

Stored User Names and Passwords is a new feature in Windows XP that stores account credentials for resources. Windows XP contains both graphical user interface (GUI) and the command line versions. It stores credentials for only integrated authentication packages in Windows XP such as NTLM, Kerberos, Passport.NET, and

SSL authentication. The types of credentials that Stored User Names and Passwords feature manages are:

- User names and passwords
- X.509 certificates (smart cards)
- Passports

These credentials are stored until needed ensuring that one guessed or stolen password does not compromise all security. If an intruder is able to determine one password that is stored by Stored User Names and Passwords he is limited to the damage he can do with that single password. One way of limiting the damage is to use different credentials for different resources.

Because the cached credentials are stored in local machine, for domain accounts it might not be a good idea to allow the use of Stored User Names and Passwords. These credentials become a part of a user's local profile in the *\Documents and Settings\Username\Application Data\Microsoft\Credentials* directory and roam with the user. Stored User Names and Passwords do not remove the risk of using weak passwords. Even though they are encrypted they might be compromised.

Allow logon through terminal services: This setting allows a user to log on to a local computer through a Remote Desktop connection. Administrators and Remote Desktop Users can access the local computer by default using Remote Desktop.

Deny logon through terminal services: This setting prevents a user or group from logging on as a Remote Desktop client. No one is denied by default.

By the two settings described above, Remote Desktop connection permissions can be set, so that only the permitted users can connect to remote computers.

Smart card removal behavior: This setting is used to configure one of the following behaviors if a smart card is removed in the middle of a session:

- Lock workstation
- Force Logoff

- No action.

b. Crypto Settings

Use FIPS compliant algorithms for encryption: This policy is used to configure available encryptions in Windows XP. This setting limits the TLS / SSL Security Provider to support only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite if enabled. In this case Windows XP will use [Ref. 13]:

- TLS protocol as a client and as a server (if applicable)
- Triple DES encryption algorithm for the TLS traffic encryption
- RSA public key algorithm for the TLS key exchange and authentication
- SHA-1 hashing algorithm for the TLS hashing requirements

By default, the Encrypting File System Service (EFS) uses the DESX algorithm, which is a strong version of DES, for encrypting file data. It is disabled by default. Enabling this setting would force it to use Triple DES.

c. Anonymous Connection (Null Session) Settings

Windows XP has also introduced a number of very specific anonymous connection (null session) restrictions. Previously there was only one setting in the Local Security Policy to control the anonymous access behavior. Now anonymous access can be explicitly defined by several settings:

Allow anonymous SID/Name translation: This setting is used to configure if an anonymous user can retrieve account security identifiers (SID) or account name for another user through an anonymous connection. If this policy is enabled, Anonymous users can retrieve the SID for any account by providing the account name or the account name by providing the SID. The combination of well-known account names might allow a connection to retrieve a SID. Using a SID-walking programs, (like UserDump [Ref. 23]) an authenticated connection could retrieve all the user names in a domain, including the administrator even if it was renamed. Even a user with knowledge of an administrator's SID could get the administrator's name by accessing a computer that has this policy enabled. The SID of administrator can be obtained by using authenticated

access to Windows XP, if Windows XP is running SMB services. This setting is disabled on workstations but enabled on server.

Do not allow anonymous enumeration of SAM accounts: This policy is used to determine if an anonymous user can retrieve the accounts that are stored in the SAM file. By default, an anonymous user has the same privileges as Everyone group and can access the SAM file. By configuring this setting, the following restrictions can be set for anonymous connections [Ref. 13]:

- ***None:*** Anonymous users can access to resources.
- ***Do not allow enumeration of SAM accounts:*** This option prevents anonymous users to access the SAM accounts by removing **Everyone** from the security permission properties of an object**.**

This policy is enabled on workstations and disabled on servers. Enabling this setting will prevent SAM accounts to be retrieved by anonymous users.

Do not allow anonymous enumeration of SAM accounts and shares: In addition to the previous setting which prevents anonymous users from accessing SAM accounts, this setting can prevent anonymous users from accessing network shares. By default anonymous user can access network shares. [Ref. 13]

This policy is disabled by default. But it should be enabled for restricting anonymous users enumerating network shares.

Let Everyone permissions apply to anonymous users: This setting is used to determine if "Everyone" permissions are applied for anonymous connections. In Windows XP the **Anonymous** users are no longer a member of the **Everyone** group. Anyone who accesses a computer and its resources through the network using anonymous connection will be granted only Anonymous group permissions. In previous versions of Windows, anonymous user had access to many resources only intended for authenticated users due to the Everyone group permissions.

By default, the "Everyone" security identifier (SID) is removed from the anonymous token. Thus, anonymous users no longer have permissions granted to the Everyone group and they can only access those resources that they were given explicit

permission. If this policy is enabled, the Everyone SID is added to anonymous token and anonymous users can access any resources which Everyone group can access. This policy setting is disabled by default.

Named Pipes that can be accessed anonymously: This setting selectively determines which communication sessions (pipes) will be accessed using anonymous connections. It is not set by default.

Shares that can be accessed anonymously: Determines which network shares can be accessed by anonymous connections. This policy setting is not set by default.

By using these anonymous connection settings, many of the attacks generated using anonymous access such as host and NetBIOS enumeration can be eliminated. Since anonymous enumeration of the shares is not disabled by default it imposes a big security risk for client computers.

d. System Object and Device Settings

Default owner for objects created by members of the administrators group: This setting is used to determine whether the Administrators group or object creator is the default owner of an object. By default the individual owns the object he created.

Prevent users from installing printer drivers: This security setting determines who is allowed to install a network printer driver to local computers. This setting only affects the network printer drivers that are installed on local printers and can be used to prevent untrusted printer drivers to be installed on local machines. If this setting is enabled, only Administrators and Power Users can install a printer driver to local computers. This setting is disabled by default. Thus any user can install printer drivers to local machines.

2. Vulnerability Scan

Vulnerability scanning is a method used for scanning networks or individual computers for vulnerabilities that attackers exploit. There are a lot of successful tools to

scan networks for vulnerabilities. As described earlier we used three of these tools. Table 8 summarizes the specifications of the computers that were scanned.

The first scan was made after a clean installation of Windows XP. The second scan was made after applying updates and patches that were released by the date scan was made. The follow-up scans were made after applying security templates. The default settings were scanned before joining a domain.

After joining a domain, the first template that was applied to Windows XP workstation was the Compatible (Compatws.inf) predefined template. The Default security (Setup security.inf) template is not applied using Group Policy. The workstation is a part of a domain and uses the settings that were defined in Group Policy in domain controllers. The Secure (Secure*.inf) and Highly Secure (hisec*.inf) templates were applied incrementally.

In this scan we especially looked at open ports and default services. Other results such as shares and registry keys are not discussed here. Account policy scan results are directly related to the template that is applied.

The same ports were observed to be open for all the templates. These ports and services they provide are described below. The differences are reflected in the Security Settings and User Rights sections for these templates. These differences are listed in Appendix C.

Windows XP supports file and printer-sharing by using the Server Message Block (SMB) protocol without using NetBios over TCP/IP. But it still supports NetBIOS as an alternative to SMB due to the need for backward compatibility. This allows Windows XP to function properly with operating systems such as Windows 95 and Windows 98 that do not support SMB. [Ref. 13]

This setting can be disabled and all SMB traffic can be forced to be direct-hosted. When NetBIOS is disabled, Windows XP will be unable to communicate with earlier operating systems using SMB traffic. If the network is completely comprised of Windows 2000 and Windows XP computers it is better to disable NetBIOS over TCP.

But direct-hosted SMBs cannot be disabled in Windows without completely disabling File and Printer Sharing for Microsoft Networks [Ref. 13]

The following ports are associated with file sharing and server message block (SMB) communications [Ref. 13]:

- Microsoft file sharing SMB: User Datagram Protocol (UDP) ports from 135 through 139, and Transmission Control Protocol (TCP) ports from 135 through 139.
- Direct-hosted SMB traffic without network basic input/output system (NetBIOS) uses port 445 (TCP and UDP).

Whichever templates are applied these ports are always open:

135/TCP RPC-LOCATOR - RPC (Remote Procedure Call) Location Service: This port is also called as end-point mapper. Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details. When trying to connect to a service, this mapper finds where it is located.

***139/TCP* NETBIOS-SSN - NETBIOS Session Service:** NetBIOS Session Services (NetBIOS Session Services are part of the NetBIOS over TCP/IP (NetBT) family of protocols and is used for server message block (SMB), file sharing, and printing.

445/TCP and ***445/ UDP* MICROSOFT-DS - Microsoft-DS:** Ports used for Direct-hosted SMB traffic without network basic input/output system Net BIOS.

1025/TCP – This is the first dynamically assigned port for outbound connections when Windows XP started.

5000/TCP and ***UDP 1900:*** Universal Plug and Play service uses these two ports. The SSDP Discovery Service is listening on this port.

3. Default Services

Most Windows applications run in the security context of the user who starts them, but many Windows services are launched by the service controller when the computer is started. Services continue to run after the

last human user logs off and they have to log on to accounts to access domain resources. [Ref. 13]

Before starting a service, the service controller logs on to the account designated for the service and presents the service's credentials for authentication by the LSA. For example, when a Windows XP Professional computer joins a domain, the messenger service on the computer connects to a domain controller and opens a secure channel to it. To obtain an authenticated connection, messenger must have credentials that the remote computer's LSA trusts. LSA uses the credentials for the local computer's domain account, as do all other services running in the security context of the Local System. [Ref. 13]

With a clean installation of Windows XP, the Setup security template is applied to computer. See Table 12 below for services that start with this template enabled. Some of these services are new and some are not required for the operating system. Disabling unnecessary services that are not needed for regular operations helps improve security throughout the organization. Some of the services are critical, such as Security Account Manager that stores security information for local computers. Disabling these critical services might prevent the system from operating.

Service Display Name	Executibale	Service Name
Application Management	svchost.exe	AppMgmt
ClipBook	Clipsrv.exe	ClipSrv
Computer Browser	Svchost.exe	Browser
DHCP Client	Svchost.exe	Dhcp
Distributed Link Tracking Client	Svchost.exe	TrkWks
DNS Client	Svchost.exe	Dnscache
Event Log	Services.exe	Eventlog
IPSEC Services	Lsass.exe	PolicyAgent
Logical Disk Manager	Svchost.exe	dmserver
Messenger	Svchost.exe	Messenger
Net Logon	Lsass.exe	Netlogon
Network DDE	Netdde.exe	NetDDE
Network DDE DSDM	Netdde.exe	NetDDEdsdm
Plug and Play	Services.exe	PlugPlay
Print Spooler	Spoolsv.exe	Spooler
Protected Storage	Lsass.exe	ProtectedStorage
QoS RSVP	Rsvp.exe	RSVP
Remote Access Connection Manager	Svchost.exe	RasMan
Remote Procedure Call (RPC)	Svchost.exe	RpcSs
Remote Registry	Svchost.exe	RemoteRegistry
Removable Storage	Svchost.exe	NtmsSvc
Secondary Logon	Svchost.exe	seclogon
Security Accounts Manager	Lsass.exe	SamSs
Server	Svchost.exe	lanmanserver
System Event Notification	Svchost.exe	SENS
Task Scheduler	Svchost.exe	Schedule
TCP/IP NetBIOS Helper	Svchost.exe	LmHosts
Windows Time	Svchost.exe	W32Time
Workstation	Svchost.exe	lanmanworkstation

Table 12: Default Services in clean installation

The significant services are as follows:

- The ***Alerter*** Service is used to broadcast administrative alerts. Alerter sends warnings about security, access, and user session problems; and therefore open up an opportunity for social engineering techniques [Ref. 18]. It is not required and must be disabled on security sensitive systems.
- ***Messenger*** Service transmits pop-up messages (as a way of simple communication between users using ***net send*** command) and Alerter service messages between clients and servers. Both Alerter and Messenger services must be disabled on machines using NetBIOS to prevent user credentials from appearing in remote NetBIOS Name Table dumps [Ref. 22].
- If ***Task scheduler*** service is not used it should be disabled. The task scheduler is often used in malicious programs such as Trojan or worms. It has also been used to access Administrative privileges [Ref. 18].
- Universal Plug and Play functionality is provided by the ***SSDP Discovery*** Service. The SSDP service enables discovery of UPnP devices. This service is not needed unless there is a new device to be connected.

Some other services that are enabled by default are not needed for everyday use. These services such as ClipBook Service, Background Intelligent Transfer Service, Automatic Updates Service, and Application Layer Gateway Service may be disabled or started manually whenever needed.

There is also a special service named “Svchost.exe”, which is actually a process name that groups services running the same dynamic-link libraries (DLLs). Each Svchost.exe process can contain a group of services. Thus multiple instances of Svchost.exe run at the same time as seen on Table 12.The Svchost.exe file is located in the %SystemRoot%\System32 folder. [Ref. 13]

Like other objects, each service has permissions (see Table 13) that can be granted or denied for accounts. These permissions can be set for services by using Security Templates and Security Configuration Tools.

Permissions	Capabilities
Full Control	Perform all functions. This permission automatically grants all service permissions to the user.
Query Template	Determine the configuration parameters associated with a service object.
Change Template	Change the configuration of a service.
Query Status	Access information about the status of the service.
Enumerate Dependents	Determine all of the other services that are dependent on the specified service.
Start	Start a service.
Stop	Stop a service.
Pause and Continue	Pause and continue the service.
Interrogate	Report the current status information for the service.
User-Defined Control	Send a user-defined control request, or a request that is specific to the service, to the service.
Delete	Delete a service.
Read Permissions	Read the security permissions assigned to the service.
Change Permissions	Change the security permissions assigned to the service.
Take Ownership	Change a security key or change permission on a service that is not owned by the user.

Table 13: Service permissions (after [Ref. 13])

A complete list of services and their descriptions can be found in Appendix D.

Service Security Contexts: Services normally run in security contexts known as Local System, Network Service, or Local Service. Windows XP has introduced Local Service, and Network Service security contexts in addition to Local System:

> ***Local Services*** have only limited local privileges, and do not need network access. When services running as Local Service access local resources, they do so as members of the local Users group. [Ref. 13]
>
> Local Service accounts access network resources using anonymous connections
>
> ***Network Services*** have no need for extensive local privileges but do need authenticated network access. A service running as Network Service has the same network access as a service running as System, but has significantly reduced local access. When services running as Network Service access local resources, they do so as members of the local Users group. When they access network resources, they do so using the SID assigned to the computer. [Ref. 13]

These accounts are important because services must log on to the computer in order to access resources. Most of the services log on to the Local System account by default on startup. Local System account is a very powerful account and it has full access to the local system. A compromised service can access to the entire domain if it logs on to the Local System account on a domain controller computer. It is very important that domain controller be protected. Other services simply log on to Local Service or Network

Service accounts which have similar permission levels as users. They must be configured to use these services in order to protect the entire system if one service is compromised.

By using Local Service and Network Service accounts, the damage will be less if one of the service accounts is compromised. However, many services still run under Local System by default. To limit the potential security risks unused or non-critical services should be stopped. Starting behaviors can be configured in Services snap-in for local machines and in Group Policy for domain computers. Noncritical services can be modified such that they start manually instead of automatic.

C. OTHER SECURITY ISSUES

1. Remote Desktop Security Issues

Remote Desktop is a new remote management feature in Windows XP. It is based on Remote Desktop Protocol (RDP) for Terminal Services. The Remote Desktop connection uses TCP port 3389. Unlike Remote Assistance or Terminal services, only one connection is allowed at the same time. When the connection is established the remote machine is locked and the user is logged out. If the user logs back on at the remote computer, the connection is terminated. Like other remote connections, the listening port for Remote Desktop is always on, and has the risks of the same type of attacks. But unlike terminal services the listening port can be changed to another port easily to leverage the security of connection. Some of the security considerations when using this new service are as follows [Ref. 24]:

a. Improper Account Permissions

A big mistake would be to make the connection with the Administrator account. This account, if compromised, can give the intruder full access to the computer and network resources. An account with administrative-level privileges should not be used in remote desktop connections.

b. Weak Passwords

Choosing weak passwords is another security risk in remote desktop connections. Weak passwords can easily be compromised and cracked by attackers. Users can setup accounts with blank password but they will not be able to connect to the host with those accounts.

c. Connecting Local Drives

When connecting to the host, the user has the option of connecting local disk drives and local ports to the remote computer. With these options enabled, the user can transfer and access the files on both the local and remote computers. In addition, users can use the programs in the remote computer and save the files to local computer.

But enabling these options may also open the ways for attackers. An infected file containing a worm, a Trojan or a virus can also connect to local computer from the remote computer.

d. ActiveX Components

In Remote Desktop Web Connection, the ActiveX component is needed to make a connection to the remote computer. For successful connection the user must hit the **Yes** button in the security warning window. Users usually tend to accept the warning without reading. It is possible that this warning can be a spoofed authentication.

e. Saving Connection Information

There is an option in the Remote Desktop connection dialog box to save the connection settings. When it is checked it speeds up connection time. But it is also a security threat. It is checked by default and the settings are stored as **default.rdb** in the **My Documents** folder. Malicious software can reach this information easily. The file contains significant information including username and password.

The Remote Desktop feature can be disabled or enabled by using Group Policy for the computers in the domain.

2. Remote Assistance Security Issues

Remote Assistance basically allows support personnel to provide remote technical support enhanced with visual and real-time communication. It needs an e-mail program or an MSN (or Windows) messenger account to send the invitation. Remote Assistance is turned on by default and uses TCP port 3389. Support technicians can have full control of the remote machine with Remote Assistance. With this kind of power, Remote Assistance has some potential security risks. Remote Assistance program can be used like a Trojan horse to gain access to the remote computer.

In order to initiate Remote Assistance, the remote machine sends an invitation to the support technician. A misconfigured invitation can lead the remote computer to be compromised by an attacker.

The support technician or helper can make important changes in the remote computer. If the connection is compromised by an attacker, a backdoor could be installed. Some important security risks associated with Remote Assistance are as follows:

- Attackers can implement fake a Remote Assistance program containing Trojan or viruses and send it to users.
- Sending invitations with weak passwords or without passwords.

These are only the potential problems specific to Remote Assistance. But other security risks can arise from poorly configured settings and network problems. Like Remote Desktop, Remote Assistance also can be disabled or enabled by using Group Policy for the computers in the domain.

3. Automatic Updates

Automatic updates also can be dangerous, for instance they can cause the system to crash or to expose another security hole. It is safer to test these updates comprehensively before applying them to workstations in an organization.

4. Passport and .Net

Microsoft Passport is a new feature in Windows XP. Any user who uses Windows Messenger is asked to sign up for a Windows .NET passport in the initial launch of Windows XP.

Most users in an organization probably will not be using Windows Messenger or similar programs. It is embedded in Windows XP and to disable it or uninstall from computer takes some effort because this service is hidden and can't be uninstalled without configuring "sysoc.inf" in "Windows/inf" folder. The "HIDE" word must be deleted in the corresponding Messenger setting in this file. After this is done Messenger service is available for uninstalling by the "Add Remove Windows Components" snap-in. The major problem with Passport is privacy. Passport stores personal information about who signed up for the service.

5. Raw Sockets

Raw sockets basically take packets, bypass the normal TCP/IP processing, and send them to the application that requests them. The user who has access to raw sockets also has access to the address fields of the IP headers in packets. If the machine is ever compromised, the attacker can gain Administrator privileges and access to the raw sockets. They then can change the IP headers and send data across the network with fake return IP addresses. This kind of attack is commonly known as "spoofing" and used in Denial of Service (DoS) attacks in which millions of packets targeted a host leaving it unable to answer to legitimate traffic.

Windows XP has the ability to write these raw IP packets. But only users who have Administrator privileges can access the raw sockets functionalities. There is no additional risk in domain based networks due to the raw socket functionality in Windows XP, as long as Administrator account is not compromised.

6. Internet Connection Firewall

The main limitation to ICF is that it does not perform outbound packet filtering other than checking the source IP address. A malicious program can send information without knowledge of the user.

ICF can examine the headers of outbound packets to ensure that an incorrect source address was not put in the stack. This will prevent spoofed DoS attacks to be originated from that machine.

7. File Encryption

Encryption File System (ECF) is an improvement over Windows 2000 operating system. Windows XP has improved ECF in several ways [Ref. 13]:

- Enabled by default
- Enhanced encryption support for cached (offline) files
- Allowed multiple users to access an encrypted document
- Supported file sharing with Web Developing Authoring and Versioning (WebDAV)

Because encryption is only available on an NTFS volume, encryption is lost when an encrypted file is copied to a FAT or FAT32 volume. If encryption is made at the file level, the plain-text temporary files could remain on the drive. In order to prevent this, encryption should be made on folder levels. Also higher privileged user might decrypt the file and folders by using EFS. If some privileged accounts are compromised, encrypted files can be viewed.

When an encrypted file is copied through the network the destination computers' encryption settings are important. If the remote computer doesn't allow encryption the file will loose its encryption. The remote encryption is not enabled by default. When a user opens an encrypted file over the network, the file is decrypted on the remote machine and transmitted as plain-text across the network. To ensure security, some other secure protocols such as Secure Socket Layer (SSL) must be used. Users also can use Web Distributed Authoring and Versioning (WebDAV) for accessing remote files. WebDAV allows using HTTP to access files remotely through firewalls, by maintaining encryption while transmitting them through public networks. When accessing to remote files stored on Web Folders the file decryption occurs on local computer. Thus, the file remains encrypted during transmission across network

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS FOR WINDOWS XP SECURITY

A. INTRODUCTION

Windows XP introduced many new features to improve performance and security over Windows 2000. There are many new security related settings included with Windows XP. It has also some new features that pose additional security risks to the user. When these features are used or configured unintelligently they might cause security risks. This chapter will address how Windows XP can be configured for enterprise wide security by using security settings. These settings will be in the form of a security template and can be deployed for all the Windows XP and Windows 2000 machines on the network. Some of the settings are not applicable to Windows 2000 workstations and they will be ignored in these machines. In addition there are some other security settings that cannot be configured via a security template. These recommended settings will be addressed separately.

B. SECURITY SETTINGS USING TEMPLATES

The following template can be deployed to any Windows XP and Windows 2000 Professional workstations using Domain Security Policy snap-in in Windows 2000 Advanced Server domain controller. This snap-in is an extension of Group Policy.

These settings are derived from the best of the Windows XP security templates and the analysis made in previous sections. These settings should be applied to workstations in domain environments that do not store security sensitive information.

1. Password Policy

Configurable Item	Recommended Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

2. Account Lockout Policies

Configurable Item	Recommended Setting
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

3. Audit Policy

Configurable Item	Recommended Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

4. User Rights Assignment

Configurable Item	Recommended Setting
Access this computer from the network	Administrators, Users
Act as part of the operating system	None
Add workstations to domain	None
Adjust memory quotas for a process	Administrators
Allow logon through Terminal Services	Administrators
Back up files and directories	Administrators
Bypass traverse checking	Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	None
Deny access to this computer from the network	None
Deny logon as a batch job	None
Deny logon as a service	None
Deny logon locally	None
Deny logon through Terminal Services	None
Enable computer and user accounts to be trusted for delegation	None
Force shutdown from a remote system	Administrators
Generate security audits	None
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	None
Log on as a batch job	None
Log on as a service	None
Log on locally	Administrators, Users
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	None
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators, Users
Replace a process level token	None

Configurable Item	Recommended Setting
Restore files and directories	Administrators
Shut down the system	Administrators, Users
Synchronize directory service data	None
Take ownership of files or other objects	Administrators

5. Security Options

Configurable Item	Recommended Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Rename to something not easily guessed
Accounts: Rename guest account	Rename to something not easily guessed
Audit: Audit the access of global system objects	Enabled
Audit: Audit the use of Backup and Restore privilege	Enabled
Audit: Shut down system immediately if unable to log security audits	Enabled
Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Do not allow installation
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	Not defined
Domain member: Require strong (Windows 2000 or later) session key	Disabled (Enable if all systems on the network require 128-bit session key)
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 logons

Configurable Item	Recommended Setting
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Not defined
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	30 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	None
Network access: Remotely accessible registry paths	Default
Network access: Shares that can be accessed anonymously	None
Network access: Sharing and security model for local accounts	Classic
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require message integrity
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require message integrity
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled

Configurable Item	Recommended Setting
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Enabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Default owner for objects created by members of the Administrators group	Object Creator
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

6. Event Log

Configurable Item	Recommended Setting
Maximum application log size	4194240 kilobytes
Maximum security log size	4194240 kilobytes
Maximum system log size	4194240 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	7 days
Retain security log	7 days
Retain system log	7 days
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually

This template eliminates or mitigates most of the vulnerabilities and risks previously discussed in this study.

C. SECURITY RECOMMENDATIONS FOR OTHER FEATURES

These additional steps will augment the above template and improve Windows XP's security posture on the network.

1. Encryption

When users encrypt their data, it is accessible only from their account. Other users have no access to this data. It is very important that users back-up private/public keys along with any certificates to a removable media. If user forgets the key, there is usually no known method to recover it. In addition, the partition that stores the key pair might crash. To prevent this, Administrators should create Recovery Agents for key recovery.

- Exporting the private keys for recovery accounts, storing them in a safe place on secure media, and removing the keys from computers prevents

someone from using the recovery account on the computer to read files that are encrypted by others.

- It is more convenient to encrypt folders instead of files. Otherwise there is a risk that plain-text temporary files might leave on the hard drive.
- Because FAT volumes do not support encryption, it is better to format all partitions with NTFS. When an encrypted file is moved or copied to an FAT partition it loses its encryption.
- For offline file accessing users should use Web Folders (WebDAV) instead of network shares. They are easier to manage and more secure. This ensures that the data is encrypted during transmission.

2. Internet Connection Firewall (IFC)

IFC is a basic firewall intended for home users who have nothing else to protect them while they are connected to Internet. For users operating in a managed domain environment, there is no perceived benefit to enabling this functionality.

3. Remote Desktop

Remote Desktop a remote control program using terminal services. Users can connect to their Windows XP desktops over any TCP/IP network remotely. In order to use properly and securely some guidelines must be followed:

- Administrator account should not be used in connections.
- The same password policies should be applied to accounts that are used in Remote Desktop connections.
- Unless needed it is better to give the least privileges to connections. For example enabling to connect local drives and ports may help a Trojan or virus to infect remote or local computers.

4. Remote Assistance

Since the support technician has full control of the local machine with Remote Assistance, this might cause security risks. In corporate networks there might no need for

Remote Assistance. Unless needed it should remain disabled. But if enabled some guidelines must be followed for secure connections:

- Users should not open Remote Assistance request unless they are completely sure of the identity of sender.
- Users must use strong passwords for Remote Assistance invitations.
- There must always be a time limit for connections. This helps reduce the risk of abuse if the connection is compromised.
- Remote Assistance should not be used in security-sensitive computers.

D. AREAS FOR FURTHER STUDY

Although registry and file system settings are set in pre-defined Windows XP templates we didn't include them in the recommended template. One area of research would include a study of these settings and which ones should be included in our recommended template.

Another potential area for further study is Microsoft's new server operating system Windows.NET Server. Windows.NET Server is currently in its Release Candidate One build, and is due for final release in late 2002 or 2003 beginning. It is very similar to Windows XP in terms of user interface and supported technologies. In addition it adds a lot of new features to Windows 2000 Advanced Server. But because it is a new operating system and contains additional features and source code, it may contain additional settings and policies. Microsoft also delayed its official release in order to make it more secure. These new settings and policies should be examined in detail. This thesis did not look at these potential changes.

E. FINAL THOUGHTS

This chapter has covered recommendations for settings listed in the security template. Additionally some other recommendations were expressed separately; areas for additional study and analysis were also discussed. Because security of workstations heavily depends on Group Policy settings in Windows 2000 domains, the settings discussed here must be applied to workstations using Domain Security Policy in domain controller.

Securing Windows XP is not enough to ensure the overall security of organization; all of the workstations and servers must also be secured in the domains. Creating and applying a strong security policy throughout the organization is the first step of secure computing.

The intent of this thesis was to discuss the security of Windows XP. A bottom-to-top approach was followed to ensure that we cover every aspect of Windows XP security. From Windows XP architecture, to application settings, every security related feature was explored. At the end, a recommended security template was given to ensure a uniform level of security for organizations that deployed Windows XP operating system for workstations.

This study has not attempted to compare Windows XP security features with those of other operating systems. We do not claim that Windows XP is sufficient to provide adequate security policy enforcement for many enterprises. Our objective has been to provide guidance regarding the use of the security features available in Windows XP such that known security exposures introduced by the XP system can be reduced through appropriate configuration.

APPENDIX A: HISTORY OF WINDOWS OPERATING SYSTEMS

Microsoft first began development of the Interface Manager (later renamed Microsoft Windows) in September 1981.

A. WINDOWS 1.0

Microsoft introduced the graphical interface of Windows 1.0 first in 1985. The first prototypes used menus at the bottom of the screen; the interface was changed in 1986 to use pull-down menus and dialogs. But there were only limited number of supported applications at that time. Due to this shortage, Windows was used as a runtime environment for some applications. Windows 1.0 provided an easy-to-use graphical user interface, device-independent graphics and multitasking support. [Ref. 6]

B. WINDOWS 2.0

Windows 2.0 was introduced in the fall of 1987, with significant GUI improvements. Adding icons and overlapping windows to the operating system, Windows then became a workable platform for major applications (such as Excel, Word, Corel Draw, and PageMaker). In late 1987 Microsoft released Windows/386. While it was functionally equivalent to Windows/286 it provided the capability to run multiple DOS applications simultaneously in the extended memory.

C. WINDOWS 3.0

Each new version of Windows extended the capability and limits of CPU speed, memory capacity, and disk space. Early versions of Windows had problems with hardware and software. The computer industry and users didn't really pay attention until Windows 3.0 was released, in 1990, as the PC operating system. It had new features like a colorful interface, the capability to address memory beyond 640K, cooperative multitasking, and a comprehensive API for developers. Windows 3.0 immediately dominated the market with widespread third-party hardware and software support. But stability still was a problem. Windows 3.0 was known to have stability problems. [Ref. 6]

D. WINDOWS 3.1

Microsoft released Windows 3.1 in 1992. It contained numerous bug fixes, added a few new features, including scalable TrueType fonts and was more stable. Windows 3.1, a 16-bit OS, had little inter-application protection. It was very easy for one application to unintentionally access another application's memory space; causing crashes and security problems. [Ref. 6]

Windows for Workgroups 3.1 was released in October 1992. It integrated networking and workgroup capabilities, including electronic mail delivery, group meeting scheduling, file and printer sharing, and calendar management.

E. WINDOWS NT

Windows NT was released in 1993. The project began in 1988 as OS/2 3.0 but eventually became a total rewrite of the code. Windows NT was written as a 32 bit OS from the start.

> Although it looked like Windows 3.1, the Windows NT architecture provided more security and protection from inter-application problems, by running applications in protected memory space. Applications were prevented from accessing hardware and memory resources, except when given explicit permission. The NT Kernel ran in its own protected memory space as well. Theoretically, an application could crash and not bring down the system. In addition to memory protection, a new NTFS file system offered higher levels of security. [Ref. 6]

It had also offered richer Win32 API, which made it easier to write powerful programs.

F. WINDOWS 95 AND NT 4.0

With the release of Windows 95 in 1995, consumers and corporate users were offered better networking support, better device support, and a more user-friendly platform. Win 95 also added an integrated TCP/IP stack, Dial-Up Networking, and long filename support. Microsoft designed Windows 95 in 32-bit architecture, but a large part of Windows 95 still remained 16-bit to provide backward compatibility with the DOS.

Windows NT 4.0 followed Windows 95 in 1996, featuring the Windows 95 user interface, expanded device support, and many bundled server processes. It was built on the more robust NT code base. “The main difference between NT and the Windows 95

was that NT controlled every aspect of I/O for advanced security and stability." [Ref. 6] It became the main platform for intranets and public Internet.

G. WINDOWS 98

Windows 98 was announced in 1998 (providing a better user interface, USB and 1394 support, ACPI power management, an integrated FAT-32 file system for more efficient and larger hard disk support, application load improvements and more utilities for system maintenance). Windows 98 included tools to increase stability, such as Scandisk, the Registry checker, and the disk cleanup utility. Windows 98 also improved Internet support. Internet Explorer was integrated and improved with support for DHTML and Java. It also included email, newsgroup, and web authoring clients. Another improvement was DirectX support and kernel enhancements for better audio and video playback. [Ref. 6]

H WINDOWS 2000

Microsoft launched Windows 2000 as a revision to Windows NT. Earlier versions of NT had supported CPU architectures other than x86-based processors. Windows 2000 would not provide support for any other platforms and was exactly an x86platform. Windows 2000 borrowed much of Windows 98's GUI, and supported the FAT-32 file system (in addition to NTFS), so compatibility and upgrades from Windows 98 machines was possible. Windows 2000 was easier to maintain with the Microsoft Management Console (MMC). The Active Directory file system added a DNS based file system, with LDAP directory and Kerberos authentication support. With the Win32 Driver Model, more devices were supported. Windows 2000 was the most stable in the line of NT versions. [Ref. 6]

I. WINDOWS ME

When released in 2000, Windows Me (Millennium Edition) was the last version of the old kernel. Home users could now add networking with the Home Network Wizard. Windows Me inherited the Windows 2000 TCP/IP stack for more robust Internet connectivity. It also added PC Health features with the ability to restore to previous configurations. Windows Me had stability problems inherited from previous versions. [Ref. 6]

J. WINDOWS XP

With the announcement of Windows XP, the differences between the consumer desktop and corporate code bases are gone. Windows XP Professional and Home versions are built from the same code base of Windows 2000. With this design corporate users will gain the increased

device and software compatibility of the consumer versions, without sacrificing stability and security. Consumers also benefit from the basic stability and security of the corporate versions. [Ref. 6]

Table 14 shows the minimum requirements for various Windows desktop operating systems.

REQUIREMENTS	WINDOWS 3.1	WINDOWS 95 OSR1	WINDOWS 98	WINDOWS ME	WINDOWS 2000 PRO	WINDOWS XP Home / PRO
Processor	80386 or higher processor	386 DX or higher processor	486DX/66 MHz or Higher processor	Intel Pentium 150 MHz or faster processor	Intel Pentium 133 MHz or equivalent processor	233 MHz or faster processor
Memory	2MB + RAM	4MB + RAM	16 MB RAM	32 MB RAM	32 MB RAM	128MB RAM
	8MB Hard disk drive space	35MB Hard disk drive space	Approximately 195MB; can take up to 295MB	At least 270 MB can take up to 410MB of hard disk space	650 MB Disk space	1.5GB Hard Disk space
Drives	3.5" / 5.25"Floppy	CD-ROM or Floppy	CD-ROM or Floppy	CD-ROM / DVD-ROM drive	CD-ROM / DVD drive	CD-ROM or DVD Drive
Sound		Sound Blaster compatible Sound Card.	Standard Sound card for sound capability	Sound Card with Speakers recommended	Optional	Sound Card recommended
Video	VGA	VGA or higher-resolution	VGA or higher-resolution	VGA or higher-resolution	VGA or higher-resolution	SVGA Video Card
Controls	Keyboard / Mouse	Keyboard / Mouse	Keyboard / Mouse	Keyboard / Mouse	Keyboard / Mouse	Keyboard / Mouse

Table 14: Operating systems requirements

A summarized and minimal comparison of Windows operating systems is shown in Table 15 below. A detailed comparison of these operating systems can be found in Appendix B.

FEATURES	WINDOWS 3.1	WINDOWS 95 OSR1	WINDOWS 98 / 98 SE	WINDOWS ME	WINDOWS NT / 2000 PRO	WINDOWS XP Home / PRO
Stability	Prone to crash	1. 32-Bit operating system 2.Improved memory handling processes 3.Pre-emptive multitasking and multi-threading	1.Protection for important files 2.FAT32 enhanced file system 3.System file checker	1.Protection of important system files 2. System Restore	1. Increased uptime of the system and significantly fewer OS reboot scenarios 2.Windows Installer 3.Memory protection	Fully protected memory
Security	Minimal, as these platforms are intended for the home user	Minimal, as these platforms are intended for the home user	Minimal, as these platforms are intended for the home user	Minimal, as these platforms are intended for the home user	1. Ability to place restrictions on file/folder access on a user-by-user basis. 2. Encrypted File System 3. Secure Virtual Private Networking	1. Built-in Internet Connection Firewall 2.Security management features. 3. Auto update
Software support & compatibility	Compatible with 16 bit applications	Compatible with 16 bit applications	Compatible with most (including DOS) applications	Compatible with most (including DOS) applications	Many DOS, 16-bit Windows, and Windows 95 applications will not run.	Integrated application compatibility technologies
Hardware support & compatibility	Mouse support	Improved support for new devices	Improved support for new devices such as AGP, Direct X, DVD, USB, MMX	Additional support for latest technology such as MMX, USB, Pentium III and more	1.Support for AGP, USB, DVD, IEEE 1394. Does not support EIDE drives, 5 1/4" floppies, and many older ISA bus devices (i.e., scanners) 2.Adding hew hardware without rebooting	Device and hardware support for greater system stability and device compatibility.
Networking	Can be used as networking client	1.Supports all major networking protocols 2. Built in remote administration 3.Dial-up networking	1.Peer to peer 2.Improved Dial-Up networking 3.Support for Virtual Private Networking (VPN)	1.Peer to peer 2.Improved Dial-Up networking 3.Support for Virtual Private Networking (VPN) 4.Simplified home networking	1. Client-server 2.Support for 15 networking protocols. 3.Can change network settings without rebooting 4.Interoperability with UNIX networks	Home Edition comes with simplified home networking but cannot join Microsoft Domains.
Software bundled	N/A	N/A	N/A	Windows Media Player 7, Windows Movie Maker, Outlook Express 5.5, NetMeeting 3.1	Active Directory, Outlook Express 5.5	Windows Media Player 8, Internet Explorer 6, Outlook Express XP
Plug & Play support	No	Yes	Yes	Yes	Yes	1. Support for hundreds of devices 2. Enhanced support for USB, IEEE 1394, PCI, and other buses.
Other features	Multitasking	1. Registry 2. Simplified user interface	1.Windows Update 2.Disk Defragmenter 3.Active Desktop (web-based user interface)	1.Windows Update 2.Disk Defragmenter 3.Active Desktop (web-based user interface)	1.Offline files and folders. 2. Support for FAT16, FAT32 and NTFS	1.New interface 2.Multilingual support

Table 15: Operating systems feature comparison

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: WINDOWS OPERATING SYSTEMS COMPARISON

This comparison table is an exact copy of the table available at [Ref. 25]

With the strengths of Windows 2000 Professional and the best business features of Windows 98, Windows XP Professional is the best desktop operating system for business.

A. DEPENDABLE

1. Stays Up and Running

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Built on New Windows Engine	Windows XP Professional is built on the proven code base of Windows 2000, which features a 32-bit computing architecture, and a fully protected memory model. This makes Windows XP Professional the most reliable version yet.	Feature not included	Feature partly supported/included	Feature included	Feature included
System Restore	The System Restore feature enables users and administrators to restore a computer to a previous state without losing data. System Restore automatically creates easily identifiable restore points, which allow you to restore the system to a previous time.	Feature partly supported/included (in Windows Me)	Feature not included	Feature not included	Feature included
Device Driver Rollback	When certain classes of new device drivers are installed, Windows XP Professional will maintain a copy of the previously installed driver, which can be reinstalled if problems occur.	Feature not included	Feature not included	Feature not included	Feature included
Device Driver Verifier	Building on the device driver verifier found with Windows 2000, the Windows XP Professional version will provide even greater stress tests for device drivers.	Feature not included	Feature not included	Feature included	Feature included
Dramatically Reduced Reboot Scenarios	Eliminates most scenarios that forced users to reboot in Windows NT 4.0 and Windows 95/98/Me. Also, many software installations will not require reboots.	Feature not included	Feature not included	Feature included	Feature included

Scalable Memory and Processor Support	Supports up to 4 gigabytes (GB) of RAM and up to two symmetric multiprocessors.	Feature not included	Feature included	Feature included	Feature included

2. Reduces Application Failure

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Side-by-Side DLL Support	Provides a mechanism for multiple versions of individual Windows components to be installed and run "side by side."	Feature partly supported/included	Feature not included	Feature included	Feature included
Windows File Protection	Protects core system files from being overwritten by application installations. If a file is overwritten, Windows File Protection will restore the correct version.	Feature not included	Feature not included	Feature included	Feature included
Windows Installer	An integrated service that helps users install, configure, track, upgrade, and remove software programs correctly.	Feature not included	Feature not included	Feature included	Feature included

3. Enhances Windows Security

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Internet Connection Firewall	A firewall client that can protect small businesses from common Internet attacks.	Feature not included	Feature not included	Feature not included	Feature included
Encrypting File System (EFS) with Multi-user Support	Encrypts each file with a randomly generated key. The encryption and decryption processes are transparent to the user. In Windows XP Professional, EFS can allow multiple users access to an encrypted document.	Feature not included	Feature not included	Feature partly supported/included (No support for use with multiple users)	Feature included
IP Security (IPSec)	Helps protect data transmitted across a network. IPSec is an important part of providing security for virtual private networks (VPNs), which allow organizations to transmit data securely over the Internet.	Feature not included	Feature not included	Feature included	Feature included
Kerberos Support	Provides industry-standard and high-strength authentication with fast, single sign-on to Windows 2000-based enterprise resources. Kerberos is an Internet standard, which makes it especially effective for networks that include different operating systems, such as UNIX.	Feature not included	Feature not included	Feature included	Feature included

Smart Card Support	Windows XP Professional integrates smart card capabilities into the operating system, including support for smart card login to terminal server sessions.	Feature not included	Feature not included	Feature not included	Feature included

B. SIMPLIFIED MANAGEMENT AND DEPLOYMENT

1. Simplifies Desktop Deployment

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Increased Application Compatibility	Hundreds of applications that didn't run in Windows 2000 Professional will run on Windows XP Professional, right out of the box.	Feature not included	Feature not included	Feature not included	Feature included
	If an application is not natively supported by Windows XP Professional, a user or system administrator can specify if the application needs to run in either a Windows NT 4.0 or Windows 95/98/Me compatibility mode, giving the program an opportunity to execute appropriately without a noticeable loss of performance.				
	As programs are updated for the new operating system, the updates will be available on the Windows Update Web site.				
User State Migration Tool	Helps administrators migrate a user's data and application/operating system settings from an old computer to a new Windows XP Professional desktop computer.	Feature not included	Feature not included	Feature partly supported/included	Feature included
Support for Latest Hardware Standards	Windows XP Professional supports the latest hardware standards. It supports UDF 2.01, the latest standard for reading DVD discs. It also supports the formatting of DVD-RAM drives with the FAT32 file system. DirectX® 8 API support will be included, and Windows XP Professional fully supports standards for Infrared Data Association (IrDA), Universal Serial Bus (USB), and the high-speed bus known as IEEE 1394.	Feature partly supported/included	Feature not included	Feature partly supported/included	Feature included

Setup with Dynamic Update	The Windows XP Professional Setup routine ensures that the operating system files are up to date. Before any files are installed, Windows XP Professional checks the Web for critical system updates and downloads them for installation.	Feature not included	Feature not included	Feature not included	Feature included
Unattended Installation	Provides the ability to specify a greater number of options than previous versions of Windows, and allows for a greater degree of security by encrypting passwords in the answer files.	Feature partly supported/included	Feature partly supported/included	Feature partly supported/included	Feature included
Internet Explorer 6 Administration Kit	Internet Explorer 6 is more customizable via the Internet Explorer Administration Kit (IEAK 6), so it's easier to deploy and maintain the browser. Version 6 of the IEAK adds control over new features such as the Media bar, Auto Image Resize, and the Personal bar.	Feature not included	Feature not included	Feature not included	Feature included
System Preparation Tool (SysPrep)	SysPrep helps administrators clone computer configurations, systems, and applications. A single image, which includes the operating system and business applications, can be restored to multiple different machine configurations.	Feature not included	Feature partly supported/included (Version 1.0 available as download)	Feature not included	Feature included
Setup Manager	A graphical wizard that guides administrators in designing installation scripts.	Feature included	Feature included	Feature included	Feature included
Remote OS Installation	Can be installed across the network (including SysPrep images). Note: This feature requires the Active Directory™ service.	Feature not included	Feature not included	Feature partly supported/included	Feature included
Multilingual Support	Allows users to easily create, read, and edit documents in many languages with the English version of Windows XP Professional. The Multilanguage User Interface version lets you change the user interface language for each user.	Feature not included	Feature not included	Feature included	Feature included

2. Improves Desktop Management

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Remote Assistance	Remote Assistance enables a user to share control of his or her computer with someone on a network or the Internet. An administrator or friend can view the user's screen, and control the pointer and keyboard to help solve a technical problem. IT departments can build custom solutions, on top of published APIs using HTML, to tailor Remote Assistance to their needs, and the feature can be centrally enabled or disabled.	Feature not included	Feature not included	Feature not included	Feature included
Group Policy	Group Policy settings simplify the administration of users and objects by letting administrators organize them into logical units, such as departments or locations, and then assign the same settings—such as security, appearance, and management options—to all employees in that group. There are hundreds of new policies available for Windows XP Professional, in addition to those provided for Windows 2000 Professional.	Feature not included	Feature not included	Feature partly supported/included	Feature included
Resultant Set of Policy (RSoP)	Allows administrators to see the effect of Group Policy on a targeted user or computer. With RSoP, administrators have a powerful and flexible base-level tool to plan, monitor, and troubleshoot Group Policy.	Feature not included	Feature not included	Feature not included	Feature included
Improved Help and Support Services	The Help and Support Center combines features users are familiar with from previous versions of Windows (such as Search, Index, and Favorites) with content from the World Wide Web to give users more chances to get the help they need when they need it. If the content in the Help and Support Center doesn't answer their question, it can be used to contact a friend, a support community, or a professional to get assistance. Tools such as My Computer Information and System Restore are also available to diagnose and fix common problems.	Feature partly supported/included (Subset of features in Windows Me)	Feature not included	Feature not included	Feature included

Automatic Updates	With the user's permission, Windows XP Professional automatically downloads critical and security updates in the background when the user is connected to the Internet. These downloads are designed to minimize the impact on Internet browsing, and the update automatically resumes upon reconnection if the computer is disconnected before the download is complete. Once the update has been downloaded, the user can choose to install it.	Feature partly supported/included (Subset of features in Windows Me)	Feature not included	Feature not included	Feature included
Windows Update Improvements	As application compatibility updates, new device drivers, and other updates are released for Windows XP Professional, they become available on the Windows Update Web site. (Users can also find critical and security updates here, if they choose not to use automatic updating.) Administrators can disable user access to Windows Update. The Windows Update Catalog is provided for administrators to download updates and deploy them as appropriate in their organizations.	Feature not included	Feature not included	Feature not included	Feature included
Microsoft Management Console (MMC)	Provides a centralized and consistent environment for management tools.	Feature not included	Feature not included	Feature included	Feature included
Recovery Console	Windows XP provides a command-line console for administrators to start and stop services, format drives, read and write data on a local drive, and perform many other administrative tasks.	Feature not included	Feature not included	Feature included	Feature included
Windows Management Instrumentation (WMI)	Provides a standard infrastructure for monitoring and managing system resources.	Feature partly supported/included (Subset of features)	Feature not included	Feature partly supported/included (Subset of features)	Feature included
Safe Mode Startup Options	Allows Windows XP Professional to boot the system at the most basic level, using default settings and minimum device drivers.	Feature included	Feature not included	Feature not included	Feature included

3. Increases User Efficiency

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Fresh Visual Design	While maintaining the core of Windows 2000, Windows XP Professional has a fresh visual design. Common tasks have been consolidated and simplified, and new visual cues have been added to help users navigate their computers. Administrators or users can choose this updated user interface or the classic Windows 2000 interface with the click of a button.	Feature not included	Feature not included	Feature not included	Feature included
Adaptive User Environment	Windows XP Professional adapts to the way you work. With a redesigned Start menu, the most frequently used applications are shown first. When you open multiple files in the same application, (such as multiple e-mail messages in the Outlook® messaging and collaboration client) the open windows will be consolidated under a single task bar button. To remove some of the clutter from the notification area, items that are not being used will be hidden. All of these features can be set via Group Policy.	Feature not included	Feature not included	Feature not included	Feature included
Improved Handling of File Associations	If you are trying to open a file that is not associated with any program, Windows XP Professional can send you to a Web page from which to download or purchase the right program. Also, some file types, especially media and image files, become difficult to open because they are used with many programs and their associations change. For these files, if the associated program has been uninstalled, Windows XP Professional restores associations with default programs, such as Microsoft Image Viewer. Default programs are integrated with the operating system so the files are always easy to open.	Feature not included	Feature not included	Feature not included	Feature included

Context Sensitive Task Menus	When a file is selected in Windows Explorer, a dynamic menu appears. This menu lists tasks that are appropriate for the type of file selected.	Feature not included	Feature not included	Feature not included	Feature included
Integrated CD Burning	Windows XP Professional has integrated support for burning CDs on CD-R and CD-RW drives.	Feature not included	Feature not included	Feature not included	Feature included
Easily Publish Information to the Web	Files and folders can be easily published to any Web service that uses the WebDAV protocol.	Feature not included	Feature not included	Feature not included	Feature included
DualView	A single computer desktop can be displayed on two monitors driven off of a single display adapter. With a laptop computer, a user could run the internal LCD display as well as an external monitor. There are a variety of high-end display adapters that will support this functionality for desktops.	Feature not included	Feature not included	Feature not included	Feature included
Troubleshooters	Help users and administrators configure, optimize, and troubleshoot numerous Windows XP Professional functions.	Feature partly supported/included (Partial subset of features)	Feature partly supported/included (Partial subset of features)	Feature partly supported/included (Partial subset of features)	Feature included

C. BUILT FOR MOBILE AND REMOTE USERS

1. Revolutionizes the Way Remote Users Work

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Remote Desktop	Let a user access his computer and any programs and data on it, from any computer, anywhere with network access. Using Microsoft's Remote Desktop Protocol (RDP), a user could connect over the Internet and control the powerful computer in his office, while using a low-powered computer at an airport kiosk.	Feature not included	Feature not included	Feature not included	Feature included
Credential Manager	A secured store for password information. It allows users to input usernames and passwords once, and then have the system automatically supply them.	Feature not included	Feature not included	Feature not included	Feature included

Offline Files and Folders	A user can specify which network-based files and folders she needs when she disconnects from the network. Additionally, with Windows XP Professional, offline folders can now be encrypted to provide the highest level of security.	Feature not included	Feature not included	Feature partly supported/included (Without encryption support)	Feature included
ClearType	A new text display technology that triples the horizontal resolution available for rendering text through software.	Feature not included	Feature not included	Feature not included	Feature included
Offline Viewing	Makes entire Web pages with graphics available for viewing offline.	Feature included	Feature included	Feature included	Feature included
Synchronization Manager	Lets users compare and update their offline files and folders with those on the network.	Feature not included	Feature not included	Feature included	Feature included
Enhanced Online Conferencing	TAPI based applications, such as NetMeeting® 3.1 conferencing software, will benefit from advances in audio and video streaming.	Feature not included	Feature not included	Feature not included	Feature included
	Improvements in audio conferencing include:				
	Support for new codecs to improve quality and interoperability.				
	Support for the DirectSound® API to reduce latency and improve mixing.				
	Acoustic Echo Cancellation (AEC), Acoustic Gain Control (AGC) and reduced ambient noise.				
	Improved jitter buffer control and silence suppression algorithms to reduce latency and improve quality.				
	Improvements in video conferencing include:				
	New codecs to improve quality and interoperability.				
	Support for new cameras.				
	Support for the DirectDraw® API to improve video performance.				
	Support for lip-synchronization to improve synchronization of video and voice.				
	Support for larger video sizes.				

	NetMeeting 3.1 will be able to connect with multi-point conferences hosted on Exchange 2000 Conferencing Server.				

2. Extends Laptop Capabilities

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Improved Power Management	By intelligently monitoring CPU state, Windows XP Professional can reduce the amount of power it is using. The operating system will provide more accurate data on the amount of power left, which will prevent the system from shutting down prematurely. Also, by allowing for the system to wake up as the battery nears a drained state, the computer can be put into hibernation, and save work in progress. Power management can now be set for each computer, or each user on a computer.	Feature not included	Feature not included	Feature included	Feature included
Hibernate	After a set time, or on demand, Windows XP Professional will save memory to disk, and shut the power down. When power is restored, all the applications are reopened exactly as they were left.	Feature not included	Feature not included	Feature included	Feature included
Hot Docking	Lets you dock or undock your notebook computer without changing hardware configuration or rebooting.	Feature included	Feature not included	Feature included	Feature included
Advanced Configuration and Power Interface (ACPI)	Provides the latest in power management and Plug and Play support.	Feature partly supported/included (Windows 98 & Windows Me)	Feature not included	Feature included	Feature included

3. Simplifies Networking

Feature	Feature Description	Windows 95/98/Me	Windows NT 4.0	Windows 2000 Professional	Windows XP Professional
Wireless Networking	Provides secured access, as well as performance improvements, for wireless networks.	Feature not included	Feature not included	Feature not included	Feature included
Network Location Awareness	Provides an underlying service that allows the operating system and applications to determine when a machine has changed network locations.	Feature not included	Feature not included	Feature not included	Feature included
Network Setup Wizard	Makes it easy for a small business owner to set up and manage a network. The Wizard walks through key steps, such as sharing files and printers, sharing the Internet connection, and configuring the Internet Connection Firewall.	Feature partly supported/included (Subset of features in Windows Me)	Feature not included	Feature not included	Feature included
Network Bridge	Simplifies the setup and configuration of small networks that use mixed network connections (such as Cat-5 Ethernet and wireless) by linking the different types of networks together.	Feature partly supported/included (Subset of features in Windows Me)	Feature not included	Feature not included	Feature included
Internet Connection Sharing (ICS)	Connects a small office network to the Internet, using a dial-up or broadband connection. Windows XP Professional can provide network address translation, addressing, and name resolution services for all computers on a small business network to share a single connection.	Feature partly supported/included (Win 98 SE and Windows Me)	Feature not included	Feature included	Feature included
Easier Remote Access Configuration Wizards	Guide users through the steps for setting up remote access to a network or virtual private network (VPN).	Feature partly supported/included (Windows Me)	Feature not included	Feature included	Feature included
Peer-to-Peer Networking Support	Enables Windows XP Professional to interoperate with earlier versions of Windows on a peer-to-peer level, allowing the sharing of all resources, such as folders, printers, and peripherals.	Feature not included	Feature not included	Feature not included	Feature included

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: SECURITY TEMPLATES COMPARISON

The shaded rows are new in Windows XP with respect to previous versions of Windows.

A. ACCOUNT POLICY

1. Password Policy

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Enforce password history	0 passwords remembered	Not defined	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	Not defined	42 days	42 days
Minimum password age	0 days	Not defined	2 days	2 days
Minimum password length	0 characters	Not defined	8 characters	8 characters
Password must meet complexity requirements	Disabled	Not defined	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Not defined	Disabled	Disabled

2. Account Lockout Policy

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Account lockout duration	Not defined	Not defined	30 minutes	0
Account lockout threshold	0 invalid logon attempts	Not defined	5 invalid logon attempts	5 invalid logon attempts
Reset account lockout counter after	Not defined	Not defined	30 minutes	30 minutes

B. LOCAL POLICIES

1. Audit Policy

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Audit account logon events	No auditing	Not defined	Success, Failure	Success, Failure
Audit account management	No auditing	Not defined	Success, Failure	Success, Failure
Audit directory service access	Not defined	Not defined	Not defined	Not defined
Audit logon events	No auditing	Not defined	Failure	Success, Failure
Audit object access	No auditing	Not defined	No auditing	Success, Failure
Audit policy change	No auditing	Not defined	Success, Failure	Success, Failure
Audit privilege use	No auditing	Not defined	Failure	Success, Failure
Audit process tracking	No auditing	Not defined	No auditing	No auditing
Audit system events	No auditing	Not defined	No auditing	Success, Failure

2. User Rights Assignment

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Access this computer from the network	Administrators, Backup Operators, Power Users, Users, Everyone	Not defined	Not defined	Not defined
Act as part of the operating system	Not defined	Not defined	Not defined	Not defined
Add workstations to domain	Not defined	Not defined	Not defined	Not defined
Adjust memory quotas for a process	Administrators	Not defined	Not defined	Not defined
Allow logon through Terminal Services	Not defined	Not defined	Not defined	Not defined
Back up files and directories	Administrators, Backup Operators	Not defined	Not defined	Not defined
Bypass traverse checking	Administrators, Backup Operators, Power Users, Users, Everyone	Not defined	Not defined	Not defined
Change the system time	Administrators, Power Users	Not defined	Not defined	Not defined
Create a pagefile	Administrators	Not defined	Not defined	Not defined
Create a token object	Not defined	Not defined	Not defined	Not defined
Create permanent shared objects	Not defined	Not defined	Not defined	Not defined
Debug programs	Administrators	Not defined	Not defined	Not defined
Deny access to this computer from the network	Not defined	Not defined	Not defined	Not defined
Force shutdown from a remote system	Administrators	Not defined	Not defined	Not defined
Generate security audits	Local System	Not defined	Not defined	Not defined
Increase scheduling priority	Administrators	Not defined	Not defined	Not defined
Load and unload device drivers	Administrators	Not defined	Not defined	Not defined
Lock pages in memory	Not defined	Not defined	Not defined	Not defined
Log on as a batch job	Local System	Not defined	Not defined	Not defined
Log on as a service	Not defined	Not defined	Not defined	Not defined
Log on locally	Administrators, Backup Operators, Power Users, Users, Guest	Not defined	Not defined	Not defined
Manage auditing and security log	Administrators	Not defined	Not defined	Not defined
Modify firmware environment values	Administrators, Local System	Not defined	Not defined	Not defined
Perform volume maintenance tasks	Administrators	Not defined	Not defined	Not defined
Profile single process	Administrators, Power Users	Not defined	Not defined	Not defined

Profile system performance	Administrators	Not defined	Not defined	Not defined
Remove computer from docking station	Administrators, Power Users, Users	Not defined	Not defined	Not defined
Replace a process level token	Local System	Not defined	Not defined	Not defined
Restore files and directories	Administrators, Backup Operators	Not defined	Not defined	Not defined
Shut down the system	Administrators, Backup Operators, Power Users, Users	Not defined	Not defined	Not defined
Synchronize directory service data	Not defined	Not defined	Not defined	Not defined
Take ownership of files or other objects	Administrators	Not defined	Not defined	Not defined

3. Security Options

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Accounts: Administrator account status	Not defined	Not defined	Not defined	Not defined
Accounts: Guest account status	Disabled	Not defined	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Not defined	Enabled	Enabled
Accounts: Rename administrator account	Administrator	Not defined	Not defined	Not defined
Accounts: Rename guest account	Guest	Not defined	Not defined	Not defined
Audit: Audit the access of global system objects	Disabled	Not defined	Disabled	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled	Not defined	Disabled	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled	Not defined	Disabled	Disabled
Devices: Allow undock without having to log on	Enabled	Not defined	Disabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Not defined	Administrators	Administrators
Devices: Prevent users from installing printer drivers	Disabled	Not defined	Enabled	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	Not defined	Disabled	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled	Not defined	Disabled	Disabled
Devices: Unsigned driver installation behavior	Warn but allow installation	Not defined	Warn but allow installation	Do not allow installation

Domain controller: Allow server operators to schedule tasks	Not Defined	Not defined	Not defined	Not defined
Domain controller: LDAP server signing requirements	Not defined	Not defined	Not defined	Not defined
Domain controller: Refuse machine account password changes	Disabled	Not defined	Not defined	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled	Not defined	Disabled	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Not defined	Enabled	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled	Not defined	Enabled	Enabled
Domain member: Disable machine account password changes	Disabled	Not defined	Disabled	Disabled
Domain member: Maximum machine account password age	30 days	Not defined	30 days	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Not defined	Disabled	Enabled
Interactive logon: Do not display last user name	Disabled	Not defined	Disabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Not defined	Disabled	Disabled
Interactive logon: Message text for users attempting to log on				
Interactive logon: Message title for users attempting to log on				
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	Not defined	10 logons	0 logons
Interactive logon: Prompt user to change password before expiration	14 days	Not defined	14 days	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Not defined	Disabled	Enabled
Interactive logon: Smart card removal behavior	No Action	Not defined	Lock Workstation	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Disabled	Not defined	Disabled	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Not defined	Enabled	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Not defined	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	Not defined	15 minutes	15 minutes

Microsoft network server: Digitally sign communications (always)	Disabled	Not defined	Disabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Not defined	Enabled	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Not defined	Enabled	Enabled
Network access: Allow anonymous SID/Name translation	Disabled	Not defined	Disabled	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Not defined	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Not defined	Enabled	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	Not defined	Disabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Not defined	Disabled	Disabled
Network access: Named Pipes that can be accessed anonymously	None	Not defined	Not defined	Not defined
Network access: Remotely accessible registry paths	None	Not defined	Not defined	Not defined
Network access: Shares that can be accessed anonymously	None	Not defined	Not defined	Not defined
Network access: Sharing and security model for local accounts	Not Defined	Not defined	Not defined	Not defined
Network security: Do not store LAN Manager hash value on next password change	Disabled	Not defined	Enabled	Enabled
Network security: Force logoff when logon hours expire	Enabled	Not defined	Not defined	Not defined
Network security: LAN Manager authentication level	Undefined	Not defined	Send NTLMv2 response only\refuse LM	Send NTLMv2 response only\refuse LM & NTLM
Network security: LDAP client signing requirements	Not defined	Not defined	Negotiate signing	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No requirements	Not defined	No minimum	No minimum
Recovery console: Allow automatic administrative logon	Disabled	Not defined	Disabled	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	Not defined	Disabled	Disabled

Shutdown: Allow system to be shut down without having to log on	Enabled	Not defined	Not defined	Not defined
Shutdown: Clear virtual memory pagefile	Disabled	Not defined	Disabled	Enabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	Not defined	Not defined	Not defined
System objects: Default owner for objects created by members of the Administrators group	Object creator	Not defined	Not defined	Not defined
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Not defined	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Not defined	Enabled	Enabled

C. EVENT LOG

Policy	**Setup Security Workstation (Default)**	**Compatible Workstation**	**Secure Workstation**	**High Secure Workstation**
Maximum application log size	512 KB	Not defined	Not defined	Not defined
Maximum security log size	512 KB	Not defined	5120 kilobytes	10240 kilobytes
Maximum system log size	512 KB	Not defined	Not defined	Not defined
Prevent local guests group from accessing application log	Disabled	Not defined	Enabled	Enabled
Prevent local guests group from accessing security log	Disabled	Not defined	Enabled	Enabled
Prevent local guests group from accessing system log	Disabled	Not defined	Enabled	Enabled
Retain application log	None	Not defined	Not defined	Not defined
Retain security log	None	Not defined	Not defined	Not defined
Retain system log	None	Not defined	Not defined	Not defined
Retention method for application log	None	Not defined	Not defined	Not defined
Retention method for security log	None	Not defined	As needed	As needed
Retention method for system log	None	Not defined	Not defined	Not defined

D. RESTRICTED GROUPS

Policy	**Setup Security Workstation (Default)**	**Compatible Workstation**	**Secure Workstation**	**High Secure Workstation**
Group Name	**Members**	**Members**	**Members**	**Members**
Administrators	Not defined	Not defined	Not defined	Not defined
Guests	Not defined	Not defined	Not defined	Not defined
Users	Not defined	Not defined	Not defined	Not defined

E. SYSTEM SERVICES

Policy	Setup Security Workstation (Default)	Compatible Workstation	Secure Workstation	High Secure Workstation
Alerter	Not defined	Not defined	Not defined	Not defined
Application Layer Gateway Service	Not defined	Not defined	Not defined	Not defined
Application Management	OK	Not defined	Not defined	Not defined
Automatic Updates	Not defined	Not defined	Not defined	Not defined
Background Intelligent Transfer Service	Not defined	Not defined	Not defined	Not defined
ClipBook	OK	Not defined	Not defined	Not defined
COM+ Event System	Not defined	Not defined	Not defined	Not defined
COM+ System Application	Not defined	Not defined	Not defined	Not defined
Computer Browser	OK	Not defined	Not defined	Not defined
Cryptographic Services	Not defined	Not defined	Not defined	Not defined
DHCP Client	OK	Not defined	Not defined	Not defined
Distributed Link Tracking Client	OK	Not defined	Not defined	Not defined
Distributed Transaction Coordinator	Not defined	Not defined	Not defined	Not defined
DNS Client	OK	Not defined	Not defined	Not defined
Error Reporting Service	Not defined	Not defined	Not defined	Not defined
Event Log	OK	Not defined	Not defined	Not defined
Fast User Switching Compatibility	Not defined	Not defined	Not defined	Not defined
Fax	Not defined	Not defined	Not defined	Not defined
Help and Support	Not defined	Not defined	Not defined	Not defined
Human Interface Device Access	Not defined	Not defined	Not defined	Not defined
IMAPI CD-Burning COM Service	Not defined	Not defined	Not defined	Not defined
Indexing Service	Not defined	Not defined	Not defined	Not defined
Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Not defined	Not defined	Not defined	Not defined
IPSEC Services	OK	Not defined	Not defined	Not defined
Logical Disk Manager	OK	Not defined	Not defined	Not defined
Logical Disk Manager Administrative Service	Not defined	Not defined	Not defined	Not defined
Messenger	OK	Not defined	Not defined	Not defined
MS Software Shadow Copy Provider	Not defined	Not defined	Not defined	Not defined
Net Logon	OK	Not defined	Not defined	Not defined
NetMeeting Remote Desktop Sharing	Not defined	Not defined	Not defined	Not defined
Network Connections	Not defined	Not defined	Not defined	Not defined
Network DDE	OK	Not defined	Not defined	Not defined
Network DDE DSDM	OK	Not defined	Not defined	Not defined
Network Location Awareness (NLA)	Not defined	Not defined	Not defined	Not defined
NT LM Security Support Provider	Not defined	Not defined	Not defined	Not defined
NVIDIA Driver Helper Service	Not defined	Not defined	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined	Not defined	Not defined
Plug and Play	OK	Not defined	Not defined	Not defined
Portable Media Serial Number	Not defined	Not defined	Not defined	Not defined
Print Spooler	OK	Not defined	Not defined	Not defined

Protected Storage	OK	Not defined	Not defined	Not defined
QoS RSVP	OK	Not defined	Not defined	Not defined
Remote Access Auto Connection Manager	Not defined	Not defined	Not defined	Not defined
Remote Access Connection Manager	OK	Not defined	Not defined	Not defined
Remote Desktop Help Session Manager	Not defined	Not defined	Not defined	Not defined
Remote Procedure Call (RPC)	OK	Not defined	Not defined	Not defined
Remote Procedure Call (RPC) Locator	Not defined	Not defined	Not defined	Not defined
Remote Registry	OK	Not defined	Not defined	Not defined
Removable Storage	OK	Not defined	Not defined	Not defined
Routing and Remote Access	Not defined	Not defined	Not defined	Not defined
Secondary Logon	OK	Not defined	Not defined	Not defined
Security Accounts Manager	OK	Not defined	Not defined	Not defined
Server	OK	Not defined	Not defined	Not defined
Shell Hardware Detection	Not defined	Not defined	Not defined	Not defined
Smart Card	Not defined	Not defined	Not defined	Not defined
Smart Card Helper	Not defined	Not defined	Not defined	Not defined
SSDP Discovery Service	Not defined	Not defined	Not defined	Not defined
System Event Notification	OK	Not defined	Not defined	Not defined
System Restore Service	Not defined	Not defined	Not defined	Not defined
Task Scheduler	OK	Not defined	Not defined	Not defined
TCP/IP NetBIOS Helper	OK	Not defined	Not defined	Not defined
Telephony	Not defined	Not defined	Not defined	Not defined
Telnet	Not defined	Not defined	Not defined	Not defined
Terminal Services	Not defined	Not defined	Not defined	Not defined
Themes	Not defined	Not defined	Not defined	Not defined
Uninterruptible Power Supply	Not defined	Not defined	Not defined	Not defined
Universal Plug and Play Device Host	Not defined	Not defined	Not defined	Not defined
Upload Manager	Not defined	Not defined	Not defined	Not defined
Utility Manager	Not defined	Not defined	Not defined	Not defined
Volume Shadow Copy	Not defined	Not defined	Not defined	Not defined
WebClient	Not defined	Not defined	Not defined	Not defined
Windows Audio	Not defined	Not defined	Not defined	Not defined
Windows Image Acquisition (WIA)	Not defined	Not defined	Not defined	Not defined
Windows Installer	Not defined	Not defined	Not defined	Not defined
Windows Management Instrumentation	Not defined	Not defined	Not defined	Not defined
Windows Management Instrumentation Driver Extensions	Not defined	Not defined	Not defined	Not defined
Windows Time	OK	Not defined	Not defined	Not defined
Wireless Zero Configuration	Not defined	Not defined	Not defined	Not defined
WMI Performance Adapter	Not defined	Not defined	Not defined	Not defined
Workstation	OK	Not defined	Not defined	Not defined

APPENDIX D: SYSTEM SERVICES

System Services are important parts of the operating system. Many of them start when the computer starts and run until the system shuts down. They continue working even there is no user logged on. They have privileges like users or other objects. With this functionality they can access important resources in the system. If they are not used properly they can pose security risk. If compromised, they might be used for accessing sensitive data by intruders.

The below list contains the Services in Windows XP that are available out of the box. The services that are available via Support Tools and by other means are not listed here. The shaded rows are new in Windows XP with respect to previous versions of Windows.

Service Display Name	Executable	Service Name	Service Description
Alerter	Svchost.exe	Alerter	Notifies selected users and computers of administrative alerts.
Application Layer Gateway Service	Alg.exe	ALG	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Internet
Application Management	svchost.exe	AppMgmt	Provides software installation services such as Assign, Publish, and Remove.
Automatic Updates	Svchost.exe	Wuauserv	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the
Background Intelligent Transfer Service	Svchost.exe	BITS	Uses idle network bandwidth to transfer data.
ClipBook	Clipsrv.exe	ClipSrv	Enables ClipBook Viewer to store information and share it with remote computers.
COM+ Event System	Svchost.exe	EventSystem	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model
COM+ System Application	Dllhost.exe	COMSysApp	Manages the configuration and tracking of Component Object Model (COM)+-based components.
Computer Browser	Svchost.exe	Browser	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers.
Cryptographic Services	Svchost.exe	CryptSvc	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Key Service, which helps enroll this computer for certificates.

DHCP Client	Svchost.exe	DHCP	Manages network configuration by registering and updating IP addresses and DNS names.
Distributed Link Tracking Client	Svchost.exe	TrkWks	Maintains links between NTFS files within a computer or across computers in a network domain.
Distributed Transaction Coordinator	Msdtc.exe	MSDTC	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems.
DNS Client	Svchost.exe	Dnscache	Resolves and caches Domain Name System (DNS) names for this computer.
Error Reporting Service	Svchost.exe	ERSvc	Allows error reporting for services and applications running in non-standard environments.
Event Log	Services.exe	Eventlog	Enables event log messages issued by Windows-based programs and components to be viewed in Event Viewer. This service cannot be stopped.
Fast User Switching Compatibility	Svchost.exe	FastUser Switching Compatibility	Provides management for applications that require assistance in a multiple user environment.
Fax	Fxssvc.exe	Fax	Enables sending and receiving faxes, utilizing fax resources available on this computer or on the network.
Help And Support	Svchost.exe	Helpsvc	Enables Help and Support Center to run on this computer.
HID Input Service	Svchost.exe	HidServ	Enables generic input access to Human Interface Devices (HID), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices.
IMAPI CD-Burning COM Service	Imapi.exe	ImapiService	Manages CD recording using Image Mastering Applications Programming Interface (IMAPI).
Indexing Service	Cisvc.exe	cisvc	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Svchost.exe	SharedAccess	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.
IPSEC Services	Lsass.exe	PolicyAgent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
Logical Disk Manager	Svchost.exe	dmserver	Detects and monitors new hard disk drives and sends disk volume information to Logical Disk Manager Administrative Service for configuration.
Logical Disk Manager Administrative Service	Dmadmin.exe	dmadmin	Configures hard disk drives and volumes. The service only runs for configuration processes and then stops.
Messenger	Svchost.exe	Messenger	Transmits net send and Alerter service messages between clients and servers. This service is not related to Windows Messenger.
MS Software Shadow Copy Provider	Dllhost.exe	SwPrv	Manages software-based volume shadow copies taken by the Volume Shadow Copy service.
Net Logon	Lsass.exe	Netlogon	Supports pass-through authentication of account logon events for computers in a domain.

NetMeeting Remote Desktop Sharing	Mnmsrvc.exe	mnmsrvc	Allows authorized people to remotely access your Windows desktop using NetMeeting.
Network Connections	Svchost.exe	Netman	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Network DDE	Netdde.exe	NetDDE	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers.
Network DDE DSDM	Netdde.exe	NetDDEdsdm	Manages Dynamic Data Exchange (DDE) network shares.
Network Location Awareness (NLA)	Svchost.exe	Nla	Collects and stores network configuration and location information, and notifies applications when this information changes.
NT LM Security Support Provider	Lsass.exe	NtLmSsp	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Performance Logs And Alerts	Smlogsvc.exe	SysmonLog	Configures performance logs and alerts.
Plug and Play	Services.exe	PlugPlay	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.
Portable Media Serial Number	Svchost.exe	WmdmPmSp	Retrieves the serial number of any portable music player connected to computer.
Print Spooler	Spoolsv.exe	Spooler	Loads files to memory for later printing.
Protected Storage	Lsass.exe	ProtectedStorage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
QoS RSVP	Rsvp.exe	RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.
Remote Access Auto Connection Manager	Svchost.exe	RasAuto	Creates a network connection.
Remote Access Connection Manager	Svchost.exe	RasMan	Creates a network connection.
Remote Desktop Help Session Manager	Sessmgr.exe	RDSessMgr	Manages and controls Remote Assistance. If this service is stopped, Remote Assistance will be unavailable. Before stopping this service, see the Dependencies tab of the Properties dialog box.
Remote Procedure Call (RPC)	Svchost.exe	RpcSs	Provides the endpoint mapper and other miscellaneous RPC services.
Remote Procedure Call (RPC) Locator	Locator.exe	RpcLocator	Manages the RPC name service database.
Remote Registry	Svchost.exe	RemoteRegistry	Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.
Removable Storage	Svchost.exe	NtmsSvc	Manages removable media, drives, and libraries.
Routing And Remote Access	Svchost.exe	RemoteAccess	Offers routing services to businesses in local area and wide area network environments.

Secondary Logon	Svchost.exe	seclogon	Enables starting processes under alternate credentials.
Security Accounts Manager	Lsass.exe	SamSs	Stores security information for local user accounts.
Server	Svchost.exe	lanmanserver	Supports file, print, and named-pipe sharing over the network for this computer. I
Shell Hardware Detection	Svchost.exe	ShellHWDetection	
Smart Card	Scardsvr.exe	SCardSvr	Manages access to smart cards read by this computer.
Smart Card Helper	Scardsvr.exe	SCardDrv	Enables support for legacy non-plug and play smart-card readers used by this computer.
SSDP Discovery Service	Svchost.exe	SSDPSRV	Enables discovery of UPnP devices on your home network.
System Event Notification	Svchost.exe	SENS	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
System Restore Service	Svchost.exe	Srservice	Performs system restore functions.
Task Scheduler	Svchost.exe	Schedule	Enables a user to configure and schedule automated tasks on this computer.
TCP/IP NetBIOS Helper	Svchost.exe	LmHosts	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.
Telephony	Svchost.exe	TapiSrv	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.
Telnet	Tlntsvr.exe	TlntSvr	Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers.
Terminal Services	Svchost.exe	TermService	Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers. The underpinning of Remote Desktop (including RD for Administrators), Fast User Switching, Remote Assistance, and Terminal Server.
Themes	Svchost.exe	Themes	Provides user experience theme management.
Uninterruptible Power Supply	Ups.exe	UPS	Manages an uninterruptible power supply (UPS) connected to the computer.
Universal Plug And Play Device Host	Svchost.exe	upnphost	Provides support to host Universal Plug and Play devices.
Upload Manager	Svchost.exe	uploadmgr	Manages synchronous and asynchronous file transfers between clients and servers on the
Utility Manager	Utilman.exe	UtilMan	Starts and configures accessibility tools from one window
Volume Shadow Copy	Vssvc.exe	VSS	Manages and implements Volume Shadow Copies used for backup and other purposes.
WebClient	Svchost.exe	WebClient	Enables Windows-based programs to create, access, and modify Internet-based files.
Windows Audio	Svchost.exe	AudioSrv	Manages audio devices for Windows-based programs.
Windows Image Acquisition (WIA)	Svchost.exe	Stisvc	Provides image acquisition services for scanners and cameras.

Windows Installer	Msiexec.exe	MSIServer	Installs, repairs and removes software according to instructions contained in .MSI files.
Windows Management Instrumentation	Svchost.exe	winmgmt	Provides a common interface and object model to access management information about operating system, devices, applications and services.
Windows Management Instrumentation Driver Extensions	Svchost.exe	Wmi	Provides systems management information to and from drivers.
Windows Time	Svchost.exe	W32Time	Maintains date and time synchronization on all clients and servers in the network.
Wireless Zero Configuration	Svchost.exe	WZCSVC	Provides automatic configuration for the 802.11 adapters.
WMI Performance Adapter	Wmiapsrv.exe	WmiApSrv	Provides performance library information from WMI HiPerf providers.
Workstation	Svchost.exe	lanmanworkstation	Creates and maintains client network connections to remote servers.

Controlling these services is a part of good security implementation. Unused ones might be disabled or starting behaviors might be changed to *Manual*.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Microsoft Developer Network, *Windows XP Technical Overview*, white paper, 2001, Internet (http://www.microsoft.com/windowsxp/pro/techinfo/planning/techoverview/default.asp). March 2002.

2. Microsoft Developer Network, *Managing Windows XP in a Windows 2000 Server Environment*, white paper, 2001, Internet (http://www.microsoft.com/windowsxp/pro/techinfo/administration/policy/default.asp). March 2002.

3. Russinovich, Mark and Solomon, David, *Inside Windows 2000*, Microsoft Press, 2000.

4. Russinovich, Mark and Solomon, David, *Windows XP: Kernel Improvements Create a More Robust, Powerful, and Scalable OS*, 2001. Internet (http://msdn.microsoft.com/msdnmag/issues/01/12/XPKernel/XPKernel.asp). March 2002.

5. Microsoft Developer Network, *Kernel Enhancements for Windows XP*, white paper, 2001 Internet (http://www.microsoft.com/hwdev/driver/XP_kernel.asp). February 2002.

6. Munro, Jay, *Windows XP Kernel Enhancements*, 2001, Internet (http://www.extremetech.com/article/0,2299,apn=3&s=1028&a=2473&app=1&ap=2,00.asp). 2002.

7. Intel Corporation, Intel SpeedStep, 2002, Internet (http://www.intel.com). 2002.

8. Advanced Micro Devices, AMD PowerNow!, 2002,

Internet (http://www.amd.com). 2002.

9. Transmeta Corporation, Transmeta Long Run, 2002, Internet (http://www.transmeta.com). 2002.

10. Schmidt, Jeff, *Windows 2000 Security Handbook*, Que, 2000.

11. Department of Defense, *Trusted Computer System Evaluation Criteria (TCSEC),* 1983, Internet (http://radium.ncsc.mil/tpep). 2002.

12. Common Criteria, Common Criteria for IT Security Version 2 (ISO 15408),1998, Internet: (http://csrc.nist.gov/cc/). 2002.

13. Microsoft, *Microsoft Windows XP Professional Resource Kit Documentation*, Microsoft Press, 2002.

14. Microsoft Developer Network, *What is New for Security in Windows XP*, white paper, 2001, Internet (http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.asp). March 2002.

15. Grasdal, Martin, *Configuring and Troubleshooting Windows XP Professional*, Syngress, 2001.

16. RFC 1661, *The Point-to-Point Protocol*, 1994, Internet (http://www.ietf.org/rfc/rfc1661.txt). 2002.

17. RFC 2284, *PPP Extensible Authentication Protocol (EAP)*, 1998, Internet (http://www.ietf.org/rfc/rfc2284.txt). 2002.

18. EEye Digital Security Company, 2002, Internet (http://www.eeye.com). 2002.

19. Languard Network Security Scanner, 2002, Internet (http://www.gfi.com/languard). 2002.

20. Microsoft Developer Network, Microsoft Baseline Security Analyzer, 2002. Internet (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp). 2002.

21. @Stake, L0phtcrack, 2002, Internet (http://www.atstake.com). 2002.

22. Scambray, Joel, *Hacking Windows 2000 Exposed*, Osborne, 2001.

23. UserDump, 2002, Internet (http://www.hammerofgod.com). 2002.

24. Peikari, Cyrus, *Windows.NET Server Security*, Prentice Hall, 2002.

25. Microsoft, *Windows XP Professional Comparison Guide*, white paper, 2001, Internet (http://www.microsoft.com/windowsxp/pro/evaluation/whyupgrade/featurecomp.asp). March 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Genel Kurmay Baskanligi Bilgi Sistemler Dairesi Baskanligi
   Bakanliklar-ANKARA
   TURKEY

4. K.K.K. Tayin Dairesi Baskanligi
   Bakanliklar-ANKARA
   TURKEY

5. K.K.K. MEBS Baskanligi Bilgi Sistem Dairesi
   Bakanliklar-ANKARA
   TURKEY

6. Deniz Kuvvetleri Komutanligi Kutuphanesi
   06100 Bakanliklar, ANKARA
   TURKEY

7. Kara Harp Okulu Kutuphanesi
   Bakanliklar, ANKARA
   TURKEY

8. Richard Harkins
   Naval Postgraduate School
   Monterey, California

9. Cynthia Irvine
   Naval Postgraduate School
   Monterey, California

10. Meftun Goktepe
    Ismet Pasa Mahallesi
    Nuri Tarhan Sokak No: 9
    Devrek, ZONGULDAK
    TURKEY

11. Dan Boger
    Naval Postgraduate School
    Monterey, California